JUSS-BUSS
Institutt for kriminologi og rettssosiologi
Universitetet i Oslo

Stensilserie nr. 149

Ansvar ved misbruk av elektronisk signatur etter ny finansavtalelov

Ole Martin Juul Slyngstadli

Oslo, 2022

UiO : Det juridiske fakultet

Ansvar ved misbruk av elektronisk signatur etter ny finansavtalelov

Kandidatnummer: 674

Leveringsfrist: 18. mai 2021

Antall ord: 16 310

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Samfunnet vi lever i, blir stadig mer digitalisert. Datamaskiner, mobiltelefoner og andre elektroniske hjelpemidler har bidratt til at enhver kan kjøpe varer og tjenester, gjøre økonomiske transaksjoner og stifte kreditt døgnet rundt, hjemme så vel som på reise. Et virkemiddel i digitaliseringen er bruk av ulike verktøy for å identifisere og autentisere en persons identitet og skape elektroniske signaturer. BankID er et eksempel på et slikt verktøy, som en rekke både offentlige og private institusjoner benytter seg av. Som en følge av dette, er BankID for mange blitt nærmest en nødvendighet i hverdagen, og benyttes for innlogging hos Skatteetaten, Altinn, Nav og andre offentlige tjenester, eller i arbeidslivet, eksempelvis ved innlogging i Aktørportalen for advokater. Det samme gjelder hos finansinstitusjoner. Digitaliseringen finner også sted innenfor betalingstjenester og andre finansielle tjenester, og påvirker hvordan finansinstitusjoner både kommuniserer og interagerer med sine kunder.

Denne digitaliseringen har på den ene siden bidratt til økt effektivitet, økt omsetning og enklere tilgang på kreditt. Dette er fra myndighetenes side en ønsket utvikling.[1] For bankene har det gitt en rasjonaliserings- og digitaliseringsgevinst.[2] Behandlingen, innvilgningen og utbetalingen av forbrukslån og kredittkort går i dag svært raskt. På den andre siden har dette ført til økt risiko for svindel blant annet i form av at tredjepersoner stifter kreditt i en annen persons navn uten dennes tillatelse eller kjennskap.

Spørsmålet som da oppstår, er hvordan de medfølgende negative konsekvensene av digitaliseringen skal pulveriseres, minimaliseres og fordeles mellom bank og kunde. I dag reguleres misbruk av digital signatur av alminnelig kontrakts- og erstatningsrett, som i praksis har ført til at den som er utsatt for digitalt identitetstyveri har blitt ansvarlig for finansinstitusjonens tap i mange sammenhenger. I ny finansavtalelov[3], vedtatt i desember 2020 (heretter finansavtaleloven 2020), er det imidlertid inntatt nye regler om tapsfordeling ved ugyldige digitale signaturer i avtaler om finansielle tjenester i §§ 3-19 til 3-21, som legger et større ansvar for tapet over på finansinstitusjonene.

---

1 Se Meld. St. 27 (2015-2016).

2 Prop. 92 LS (2019-2020) s. 184.

3 Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven).

Hovedregelen etter § 3-20 er at det er finansinstitusjonen som må bære tapet dersom en avtale om finansielle tjenester er inngått av en svindler gjennom opprettelse av en falsk digital signatur i en annen persons navn. Den som har navnet sitt på avtalen, kan imidlertid bli ansvarlig for hele eller deler av tapet avhengig av graden av utvist skyld. Noe forenklet vil systemet i finansavtaleloven 2020 være at pseudodebitoren, altså svindelofferet, blir ansvarlig for egenandel på 450 kroner ved simpel uaktsomhet, 12 000 kroner ved grov uaktsomhet og hele tapet ved forsett. Problemstillingen for oppgaven er å klarlegge ansvaret for tap ved misbruk av digital signatur, med fokus på å klarlegge tersklene mellom skyldgradene. De nye reglene i finansavtaleloven 2020 gjelder for alle avtaler om finansielle tjenester, men fremstillingen avgrenses til avtaler om kredittavtaler. På grunn av potensialet for stor økonomisk gevinst for svindleren er det i slike avtaler det har forekommet mest svindel i praksis.

1.2 Metode og rettskildebildet

Finansavtaleloven 2020 og forarbeidene[4] til denne er de mest sentrale rettskildene for oppgaven. Loven kan ikke fravikes til skade for forbruker, og er i så måte en forbrukerlov ment for å styrke forbrukervernet.[5] Både rettskilder og begreper vil tolkes i tråd med alminnelig juridisk metode.[6]

Finansavtaleloven 2020 er en gjennomføring av tre nye EU-direktiver, herunder det nye betalingstjenestedirektivet, (EU) 2015/2366 Payment services (PSD 2).[7][8] Direktivet opphever PSD 1,[9] og inneholder bestemmelser om ansvar ved det som nå kalles «ikke godkjente betalingstransaksjoner», som er inkorporert i lovens kapittel 4 IV. Dette er i stor grad en videreføring av finansavtaleloven 1999 § 35, som reguleres i finansavtaleloven 2020 § 4-30. PSD 2 regulerer ikke misbruk av elektronisk signatur.

---

4 Prop. 92 LS (2019-2020) og Innst. 104 L (2020-2021)

5 Se finansavtl. § 1-9 og Prop. 92 LS (2019-2020) s. 10 samt fortalen til PSD 2 avsnitt 15.

6 Eckhoff (2001).

7 Prop. 92 LS (2019-2020) s. 9.

8 Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betailngstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF.

9 Europapalaments- og rådsdirektiv 2007/64/EF av 13. november 2007 om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, og 2006/48/EF samt oppheving av direktiv 97/5/EF.

Dette betyr at §§ 3-19 til 3-21 er særnorske, og kan ikke utledes av direktivet. Bestemmelsene om misbruk av digitale signaturer er imidlertid utformet etter modell av reglene om ansvar for tap ved misbruk av konto og betalingsinstrument.[10] Problemstillingene henger nært sammen, og kan framstå som to sider av samme sak. Selv om misbruk av digital signatur ikke er regulert i direktivet, uttaler departementet at gode grunner taler for å se problemstillingene i sammenheng.[11]

Dette medfører at rettskilder i tilknytning til finansavtaleloven 1999, herunder praksis knyttet til finansavtaleloven 1999 § 35, og vurderingen av skyldgradene der, kan ha relevans for tolkningen av §§ 3-19 til 3-21.[12] Det innebærer videre at uttalelser i PSD 2 som har betydning for tolkningen av om kunden har vært uaktsom, grovt uaktsom eller forsettlig i relasjon til «ikke godkjente betalingstransaksjoner», vil ha overføringsverdi når skyldgraden skal vurderes etter § 3-20. Hvilken rolle disse kildene konkret spiller for tolkningen av reglene om digitale signaturer i finansavtaleloven 2020, vil bli behandlet løpende. Ved tolkningen av PSD 2, som et EU-direktiv, vil det måtte gjøres i lys av bestemmelsens kontekst og formål.[13]

1.3 Begreper og avgrensninger

Finansavtaleloven 2020 regulerer alle finansavtaler, herunder finansielle tjenester og misbruk i relasjon til disse, jf. § 1-1, jf. § 1-3. I § 3-20 reguleres misbruk av BankID som elektronisk signatur i relasjon til alle avtaler om finansielle tjenester for både privatpersoner og juridiske personer. Oppgaven avgrenses som nevnt til kredittavtaler, herunder forbrukslån og kredittkort, som er det praktisk viktigste typetilfellet.

Videre regulerer § 3-20 også de tilfeller hvor juridiske personer får misbrukt sin digitale signatur. Oppgaven avgrenses til privatpersoners ansvar. Dette fordi finansavtaleloven er fravikelig i næringsforhold, jf. finansavtaleloven 2020 § 1-9.

Finansavtaleloven 2020 § 3-20 andre ledd regulerer rettsvirkningen hvor rettighetshaver «ikke kunne oppdaget misbruket» og heller ikke har opptrådt «svikaktig». Femte ledd regulerer

---

10 Prop 92 LS (2019-2020) s. 183.

11 Prop. 92 LS (2019-2020) s. 173.

12 Herunder NOU 2008:21, Ot. prp. nr. 94 (2008-2009), NOU 1994:19 og Ot. prp. nr. 41 (1998-1999)

13 Haukeland Fredriksen og Mathisen (2019) s.404

virkningen av «tap som skyldes tjenesteyteren selv, noen som opptrer på tjenesteyterens vegne, eller noen som tjenesteyteren selv representerer». Dette vil jeg ikke behandle, fordi det ikke knytter seg til graden av utvist skyld på rettighetshaverens side.

Etter finansavtaleloven 2020 § 3-19 tredje ledd oppstilles det en plikt for rettighetshaveren til å varsle om misbruk «uten ugrunnet opphold». Heller ikke dette knytter seg til graden av utvist skyld hos rettighetshaveren, men heller en varslingsplikt etter at misbruket har funnet sted. Dette vil følgelig ikke vurderes.

Forutsetningen for at reglene i finansavtaleloven 2020 § 3-20 skal komme til anvendelse, er at det ikke foreligger *avtalerettslig binding* som grunnlag for å holde BankID-innehaveren ansvarlig. Det kan tenkes tilfeller hvor det er gitt fullmakt som fører til bindende avtale, hvor det vil være relevant å vurdere fullmaktens grenser. Oppgaven avgrenses mot tilfeller hvor det foreligger fullmakt eller annet særskilt rettsgrunnlag mellom svindelofferet og svindler.

Finansavtaleloven 2020 omtaler partene som «rettighetshaver»[14] og «tjenesteyter»[15] for henholdsvis den som har rett til å fremstille en elektronisk signatur (typisk innehaveren av BankID som er misbrukt) og finansinstitusjon som har utbetalt lån eller utstedt kreditt på bakgrunn av misbruk av digital signatur. Disse partsbetegnelsene brukes i det følgende.

1.4 Den videre fremstillingen

I den videre fremstillingen vil jeg først gjøre en overordnet vurdering av forhistorien bak reglene om ansvarsfordeling og hensynene som ligger bak. Dette gjøres i kapittel 2.

Jeg vil deretter, i kapittel 3, gjøre en overordnet vurdering av reglene om ansvarsfordelingen tjenesteyter og rettighetshaver. Her vil jeg vurdere uaktsomhetsnormen og hvilke plikter en rettighetshaver har.

Deretter vil det gjøres en konkret vurdering av de ulike skyldgradene. Dette gjøres i kapittel 4, hvor alminnelig uaktsomhet drøftes, kapittel 5 for den grove uaktsomheten og kapittel 6 hvor jeg tar for meg forsettskravet.

---

[14] Jf. finansavtaleloven 2020 § 3-16 bokstav b.

[15] Jf. finansavtaleloven 2020 § 1-4 tredje ledd.

Avslutningsvis vil jeg i kapittel 7 oppsummere drøftelsene, og komme med betraktninger om rettstilstanden.

2 Forhistorie og hensyn

Jeg vil i det følgende utdype om bakgrunnen for de nye reglene om tapsfordeling ved misbruk av digital signatur, samt fremheve noen sentrale hensyn som reguleringen av ansvaret skal ivareta.

Regler om tapsfordeling ved misbruk av betalingskort har eksistert lenge. I kredittkjøpsloven av 21. juni 1985 nr. 82 § 13 ble det fastsatt ansvarsregler for misbruk av kontokort. Dette ble også regulert i den såkalte «mønsteravtalen» fra 1986.[16]

Finansavtaleloven ble vedtatt i 1999 for å gi en mer helhetlig regulering av finansområdet. Formålet var å både klargjøre rettstilstanden og sikre et mer balansert og likeverdig forhold mellom kunde og bank.[17] Med loven ble forbrukervernet styrket, blant annet ved at det ble innført egenandel for kundens ansvar ved kortmisbruk.[18] Siden vedtakelsen av loven har tilbudet på og tilgangen til finansielle tjenester vokst betraktelig. Loven har med jevne mellomrom blitt oppdatert, også som en konsekvens av Norges folkerettslige forpliktelser. Reguleringen av kontraktsrettslige spørsmål knyttet til finansielle tjenester har imidlertid ikke hengt med i utviklingen.[19]

I 2009 ble betalingstjenestedirektivet (2007/64/EF) (PSD 1) gjennomført i norsk rett gjennom revidering av finansavtaleloven. Forbrukeren ble her gitt vern for uautoriserte betalingstransaksjoner, og ikke bare for misbruk av betalingskort. Tapet kunne da bli skjøvet over på banken på visse vilkår.[20] Den nye reguleringen ble utvidet til å gjelde alle betalingstransaksjoner, herunder misbruk av nettbank. Også her gikk en i retning av å utvide forbrukervernet. Bestemmelsen tok imidlertid kun høyde for misbruk i tilfeller hvor det forelå en uautorisert beta-

16 NOU 1994:19 s. 66

17 NOU 1994:19 s. 32-33, gjengitt i Ot.prp.nr. 41 (1998-1999) s. 12.

18 Ot.prp.nr. 41 (1998-1999) s. 105.

19 Prop. 92 LS (2019-2020) s. 22.

20 Jf. finansavtl. § 35, og 2007/64/EF artikkel 60 og 61.

lingstransaksjon ved bruk av betalingsinstrument, men ikke tilfeller hvor BankID ble benyttet som digital signatur for å inngå kredittavtaler i svindelofferets navn.

I svindeltilfeller ved bruk av BankID kan det skilles mellom to ulike situasjoner av misbruk. I den ene situasjonen vil uvedkommende ved bruk av BankID logge seg inn i et svindeloffers nettbank og tømme en allerede eksisterende konto. I det andre tilfellet er fremgangsmåten den samme, men BankID brukes som digital signatur for å inngå låne- og kredittavtaler med tredjepartsbank. I dette tilfellet er det altså den digitale signaturen som misbrukes, hvor svindler ved hjelp av BankID utgir seg for å være en annen og inngår kredittavtaler i dennes navn.

De sistnevnte tilfellene har da blitt løst i domstolene etter alminnelige erstatningsrettslige regler.[21] Finansinstitusjoner har påberopt seg den alminnelige culparegelen som grunnlag for å kreve sitt tap dekket av BankID-innehaveren i tilfeller av misbruk. Argumentasjonen har vært at kunden har vært uaktsom i sin håndtering av BankID, og at dette har gitt grunnlag for erstatningskrav. Dette har ført til en sprikende og utilgjengelig rettspraksis, og det har gjennomgående blitt lagt til grunn en svært streng aktsomhetsnorm.[22]

Det er flere eksempler på dette fra underrettspraksis. I en sak ble en fengselsinnsatt svindlet av sin fetter.[23] Fetteren tok opp lån i den fengselsinnsattes navn, og banken vant fram med at den innsatte var ansvarlig på erstatningsrettslig grunnlag. Svindelofferet ble ikke trodd på at han ikke visste hvordan fetteren hadde fått tilgang til BankID-brikken. Retten fant det derfor mest sannsynlig at offeret hadde gitt fetteren tilgang på både brikke og annen nødvendig informasjon og dermed forsettlig hadde brutt sine plikter etter BankID-avtalen.

I en annen sak hadde en kvinne bodd i Norge i halvannet år og hadde signert avtale om BankID. Hun kom fra et land hvor lignende betalingsløsninger ikke eksisterte, og overlot kodebrikke og passord til sin ektemann.[24] Han tok opp lån i hennes navn. Kvinnen anførte at hun ikke forstod hva BankID-avtalen gikk ut på, og at ingen hadde oversatt den til henne. Retten konkluderte med at det var uaktsomt i seg selv å undertegne en avtale hun ikke forstod, og at

---

21 Se eksempelvis TOSLO-2018-180834, LB-2014-13514 og HR-2020-2021-A.

22 Prop. 92 LS (2019-2020) s. 175.

23 LB-2014-13514.

24 LB-2016-43622.

hun ved å gi ektemannen tilgang til både brikke og passord hadde brutt pliktene etter avtalen. Hun ble følgelig holdt ansvarlig for tapet.

Også praksis fra Finansklagenemnda kan nevnes. En eldre kvinne med Alzheimers hadde fått oppnevnt hjelpeverge, noe banken visste om.[25] Det ble tatt opp lån på kroner 140 000 i hennes navn, og hun ble holdt ansvarlig for tapet. Fordi hun hadde Alzheimers, og dermed lett glemte ting, hadde hun skrevet ned passordet og oppbevarte dette sammen med BankID-brikken. Nemnda fant at kvinnen «utvilsomt har opptrådt grovt uaktsomt» både ved nedtegnelsen av passordet og oppbevaringen sammen med brikken. Nemnda la også til grunn at banken heller ikke kunne klandres da «lånesøknaden ikke gjaldt et særlig stort beløp», fordi det var ikke noe påfallende ved søknaden og at lånet kunne gjennomføres automatisk.

Det har de senere år, på bakgrunn av historiene fra rettspraksis som har kommet frem i offentligheten, pågått en debatt om praksisen, og om menneskene bak historiene bør ha et sterkere rettsvern. Spørsmålet som har blitt reist, er om tapsfordelingen også i slike tilfeller bør reguleres særskilt etter modell av reglene om uautoriserte betalingstransaksjoner.[26] Fra finansnæringen har det blitt framholdt at disse tilfellene best løses slik sakene har blitt praktisert hittil, etter alminnelige avtale- og erstatningsrettslige regler, og at en ansvarsbegrensning vil kunne virke svindeldrivende.[27]
Det har altså over lang tid funnet sted en gradvis utvikling av forbrukervernet. Det ble først innført egenandeler ved misbruk av kreditt- og debetkort. Deretter ble vernet utvidet til å gjelde betalingstransaksjoner, herunder overføringer fra nettbank. Reguleringen har skjedd gradvis ettersom lovgiver ser behovet i praksis, men hele tiden i etterkant av den teknologiske utviklingen. Når det nå innføres regulering for misbruk av digital signatur er det nettopp dette som har skjedd; reguleringen følger etter den teknologiske utviklingen. En kunne ikke nødvendigvis forutse alle svindeltilfeller, men en kunne med tiden se behovet i praksis. Den nye ansvarsreguleringen er således en naturlig forlengelse av den gradvise utvidelsen av rettsvernet til forbrukere.

---

[25] FinKN-2014-550.

[26] Se eksempelvis https://www.advokatbladet.no/id-tyveri-norsis/mener-ny-finansavtalelov-kunne-reddet-svindelofre-fra-erstatningsansvar-etter-id-tyveri/147199 Hentet 28.4.2021 og https://e24.no/naeringsliv/i/LABV74/professor-mener-id-svindel-kan-vaere-loennsomt-for-bankene Hentet 28.4.2021.

[27] Prop. 92. LS (2019-2020) s. 176.

Justis- og beredskapsdepartementet sendte i 2017 ut et høringsnotat med forslag til ny finansavtalelov.[28] Forslaget inneholdt nye regler om tapsfordeling ved misbruk av digitale signaturer, utformet etter modell av reglene om tapsfordeling ved uautoriserte betalingstransaksjoner. Tilfellene er svært like. I begge tilfeller vil svindleren måtte ha tilgang på det samme – BankID-brikke og personlig passord og personnummer – for å gjennomføre misbruket. I tillegg kommer at dersom svindler får lånesummen utbetalt til offerets eksisterende bankkonto, for så å føre summen ut, vil det være en «uautorisert betalingstransaksjon», hvor kunden er vernet. Dersom lånesummen utbetales direkte til en konto som ikke er i offerets navn, faller det utenfor gjeldende lovs virkeområde. Dette gir et vilkårlig vern, hvor svindelofferets rettsstilling avhenger av svindlers vilkårlige valg. Dette synes å være avgjørende for at lovgiver foreslo en lik regulering av misbruk i form av uautoriserte betalingstransaksjoner og inngåelse av avtaler om finansielle tjenester med falsk digital signatur.

Til tross for store protester fra finansnæringen i høringsrunden ble forslaget fra 2017, med enkelte endringer, fulgt opp med en proposisjon 29. april 2020,[29] og 1. desember 2020 ble den nye finansavtalelov vedtatt i Stortinget. Det er ikke kommet en formell avgjørelse for når loven trer i kraft, utover at dette vil skje «fra den tid Kongen bestemmer», jf. § 8-1.[30]

Forbrukerhensyn vil, på bakgrunn av forhistorien og at finansavtaleloven er å anse som en forbrukerlov,[31] stå sentralt i tolkningen av bestemmelsene. I forholdet mellom kunde og finansinstitusjon er det en betydelig maktassymetri, hvor banken er spesialisert på området, mens en alminnelig kunde sjelden er fullt ut oppdatert på lik linje. Loven søker å skape en større grad av likevekt mellom partene.

---

28 Justis- og beredskapsdepartementet (2017) – Snr. 17/4746.

29 Prop. 92 LS (2019-2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglånsdirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014.

30 I TGLOM-2020-156504 uttales det at «[e]tter det opplyste vil ny finansavtalelov tidligst tre i kraft 01.01.2020».

31 Jf. Finansavtaleloven 2020 § 1-9 (1).

Videre vil pulveriseringhensyn være sentralt.[32] For en alminnelig person kan det være svært byrdefullt å måtte bære hele tapet i svindeltilfeller. Banken kan på sin side fordele tapet på hele kundemassen, og har helt andre økonomiske forutsetninger til å bære tapet. Dette kan også gi bankene et incentiv til å innføre sikkerhetstiltak og rutiner for å sikre seg mot å utbetale lån til uvedkommende, og dermed unngå at tapet blir realisert. Det vil på sikt kunne redusere svindelomfanget.

I forarbeidene til ny finansavtalelov er det pekt på at en rettstilstand hvor gevinsten primært kommer næringen til gode, hvor det «først og fremst er kunden som skal ha risikoen for misbruk», på sikt ikke er holdbar om en ønsker å opprettholde tilliten til digitale løsninger.[33] Det har videre blitt argumentert med at en slik rettstilstand vil kunne motvirke den ønskede digitaliseringen av finansielle tjenester.[34]

De ovennevnte hensyn kan også sies å ha et innslag av rimelighets- og rettferdighetshensyn. Digitaliseringen har bidratt til at bankene har oppnådd en betydelig rasjonaliserings- og effektiviseringsgevinst, og det kan da argumenteres med at det er rimelig at de samtidig bærer en større andel av tapene.[35] Dette underbygges også av hensynet til tillit. Om risikoen knyttet til å ha noe så nødvendig som BankID er for stor, kan det bidra til at færre benytter seg av det. Dette vil igjen være i strid med den lovgivers formål og samfunnsøkonomisk effektivitet.

3 Overordnet om ansvarsfordelingen mellom tjenesteyter og rettighetshaver ved misbruk av digital signatur

3.1 Innledende bemerkninger

Hovedregelen etter § 3-20 er at tjenesteyteren kan gjøre krav gjeldende mot rettighetshaveren «i samsvar med ellers gjeldende rettsregler for misbruk av elektroniske signaturfremstillingsdata». Om det er tilfelle kan kravet «ikke overstige de egenandeler som følger av annet til femte ledd» i bestemmelsen.

---

32 Se Prop. 92 LS (2019-2020) s. 181 og Ot.prp. nr. 41 (1998-1999) s. 128 om egenandeler ved uautoriserte betalingstransaksjoner, som bygger på de samme hensynene.

33 Prop. 92 LS (2019-2020) s. 184.

34 Prop. 92 LS (2019-2020) s. 184.

35 Prop. 92 LS (2019-2020) s. 184.

Det er dermed tjenesteyteren som er ansvarlig for tap som oppstår ved misbruk av elektronisk signatur selv om rettighetshaveren er ansvarlig etter ellers gjeldende rettsregler. Bestemmelsen gir adgang til å skyve tapet over på rettighetshaveren på nærmere bestemte vilkår.

Om misbruket kunne vært oppdaget på forhånd og rettighetshaveren ikke har opptrådt svikaktig, vil rettighetshaveren måtte svare for en egenandel på inntil 450 kroner etter annet ledd. Det er vanskelig å se at annet ledd skal få noen betydning i praksis; dersom rettighetshaveren ikke kunne oppdaget misbruket på forhånd, vil det nok heller ikke foreligge ansvarsgrunnlag. I disse tilfellene er det vanskelig å se for seg hvordan rettighetshaveren kunne handlet annerledes. Oppgaven er avgrenset mot en nærmere vurdering av dette.

Om rettighetshaveren ved «grov uaktsomhet» har unnlatt å oppfylle sine forpliktelser etter § 3-19 første og annet ledd, svarer vedkommende for en egenandel på inntil 12 000 kroner. Om unnlatelsen for å oppfylle pliktene etter § 3-19 første og annet ledd skyldes at rettighetshaveren har brutt sine plikter «forsettlig», vil egenandelen tilsvare hele tapet. Det kan bemerkes at det kalles «egenandel» når rettighetshaveren er ansvarlig for hele tapet. Dette kan i seg selv virke noe misvisende, sett hen til at utgangspunktet er at hele tapet skyves over fra tjenesteyteren til rettighetshaveren. Dette kan da vanskelig omtales som en «egenandel», men hele tapet.

Hensikten med reguleringen er å begrense rettighetshaverens ansvar etter «ellers gjeldende rettsregler» og kommer til anvendelse når tapet har oppstått på bakgrunn av «misbruk av elektroniske signaturfremstillingsdata». Dermed oppstår spørsmålet om hva som er «elektroniske signaturfremstillingsdata», og hva som er «ellers gjeldende rettsregler». Om kravet ikke kan gjøres gjeldende etter «ellers gjeldende rettsregler», kommer bestemmelsen ikke til anvendelse, og tjenesteyteren kan følgelig ikke gjøre kravet gjeldende mot rettighetshaveren. Omfanget av kundens ansvar er som tidligere nevnt basert på graden av skyld, noe jeg vil komme tilbake til i påfølgende kapitler.

3.2 Bestemmelsens anvendelsesområde. Særlig om «elektroniske signaturfremstillingsdata»

Bestemmelsen vil først komme til anvendelse når «elektroniske signaturfremstillingsdata» er misbrukt for å signere kredittavtale.

En «elektronisk signatur» er en «kvalifisert elektronisk signatur i samsvar med forordning (EU) nr. 910/2014 om elektronisk identifikasjon for elektroniske transaksjoner i det indre marked og regler gitt i eller i medhold av lov om elektroniske tillitstjenester», jf. Finansavtaleloven 2020 § 3-16 første ledd bokstav a. Det er lagt til grunn i forarbeidene at BankID kan benyttes «som (…) elektronisk signering av en avtale».[36]

I lov om elektroniske tillitstjenester § 1 gjøres forordning (EU) nr. 910/2014 til norsk lov, uten nærmere regulering i loven. I direktivets artikkel 3 nr. 13 defineres «elektronisk signatur» som «unique data which is used by the signatory to create an electronic signature». Begrepet er i loven teknologinøytralt, og BankID-brikke er eksempel på et slikt verktøy – og det klart mest utbredte for å fremstille digital signatur i Norge, med 4,2 millioner brukere.[37] Etter forarbeidene er dette definert som «kvalifiserte elektroniske signaturer som er fremstilt ved bruk av kvalifisert sertifikat i et kvalifisert elektronisk signaturfremstillingssystem».[38] Det er derfor på det rene at signering med BankID-brikke er å regne som «elektroniske signaturfremstillingsdata».

3.3 Inngangsvilkår: ansvar etter «ellers gjeldende rettsregler»

Som nevnt innledningsvis kan tjenesteyteren gjøre krav gjeldende etter «ellers gjeldende rettsregler». Ordlyden gir ikke i seg selv veiledning for hvilke regler som kommer til anvendelse for erstatningsansvaret.

I forarbeidene uttales det at «ellers gjeldende rettsregler» vil «i praksis si regler om erstatningsansvar utenfor kontrakt, eller i kontrakt om det forut for misbruket eksisterer en avtale mellom rettighetshaveren og tjenesteyteren som regulerer kundens plikter for oppbevaring og håndtering av signaturløsningen».[39] Dette peker mot en uaktsomhetsvurdering etter erstatningsrettslige regler. Det kan også utledes at dersom det i forkant av misbruket foreligger en avtale som fastsetter bestemte plikter og rettigheter mellom rettighetshaveren og tjenesteyteren, altså finansinstitusjonen, vil også avtalen kunne være veiledende i vurderingen for erstatningsansvar.

---

36 Prop. 92 LS (2019-2020) s. 173.

37 https://www.bankid.no/privat/om-oss/ [Hentet 28.4.2021].

38 Prop. 92 LS (2019-2020) s. 182.

39 Prop. 92 LS (2019-2020) s. 358.

Utgangspunktet for de aktuelle tilfellene er at det er inngått en avtale. Denne er signert med elektroniske signaturfremstillingsdata fra det som tilsynelatende er en alminnelig rettighetshaver og den digitale signaturen fremstår som en bindende aksept. Når det likevel ikke er rettighetshaveren som har signert avtalen, er det avtalerettslige utgangspunktet at denne ikke er bindende.[40] En slik signering vil omfattes av de ulovfestede reglene om falsk som tilblivelsesmangel. Falsk er en sterk ugyldighetsgrunn i avtaleretten fordi «løftegiveren aldri har avgitt et løfte».[41] Tjenesteyteren kan følgelig ikke holde vedkommende ansvarlig etter den inngåtte avtalen. Kunden kan likevel bli erstatningsansvarlig. Etter forarbeidene legges det opp til en vurdering av om rettighetshaveren har «opptrådt klanderverdig».[42] Dette må forstås som en henvisning til de foran nevnte erstatningsrettslige regler.

Det alminnelige ansvarsgrunnlaget i norsk rett er culpaansvaret.[43] I erstatningsretten er det sentrale vurderingstema for culpanormen om skadevolderen har handlet forsvarlig,[44] og om vedkommende kunne og burde handlet annerledes.[45] I vurderingen av om en person har handlet uaktsomt, er det en rekke faktorer som må vurderes og «tilpasses både det aktuelle typetilfellet generelt og ut fra faktum i den konkrete saken».[46] Det vil særlig være aktuelt å vurdere hvilke handlingsnormer som er typisk på det aktuelle livsområdet det er tale om. Normen skal være objektiv og det er en «samfunnsmessig og ikke en moralsk dom» som skal felles.[47]

Det samme gjelder i kontraktsforhold, hvor culparegelen er den alminnelige erstatningsregelen.[48] Også her forutsetter ansvar at skadevolderen, i vårt tilfelle rettighetshaveren, «kunne og skulle ha handlet annerledes».[49] Det er videre tre vilkår som må være oppfylt for at rettighetshaveren skal kunne holdes ansvarlig. Det må foreligge et ansvarsgrunnlag, det må være årsakssammenheng mellom det ansvarsbetingende forhold og skaden, samt at den inntrådte

---

40 Hov (2002) s. 237.

41 Giertsen (2014) s. 170.

42 Prop. 92 LS (2019-2020) s. 358.

43 Se eksempelvis Kjelland: Erstatningsrett (2016) s. 66.

44 Nygaard (2007) s. 172.

45 Nygaard (2007) s. 174.

46 Kjelland: Erstatningsrett (2016) s. 69.

47 Hagstrøm (2011) s. 468, se også Lilleholt (2017) s. 339.

48 Hagstrøm (2011) s. 468.

49 Hagstrøm (2011) s. 468

skade må være erstatningsmessig.[50] Det som gjør vurderingen annerledes etter finansavtaleloven er at «uaktsomhet som utgangspunkt er tilstrekkelig for ansvar i kontraktsforhold».[51] I finansavtaleloven oppstilles det krav til en vurdering av klanderverdigheten, fra den uaktsomme til den grovt uaktsomme, og videre til den forsettlige. Avhengig av utvist skyld ved brudd på sine plikter økes rettighetshavers ansvar gradvis.

Ved misbruk av elektronisk signatur vil det sjelden være problematisk å konstatere at det har oppstått et tap; tjenesteyteren har utbetalt en sum penger til uvedkommende med et tap som ellers ikke blir dekket, fordi svindler i mange tilfeller er ukjent. I praksis velger da banken å gå på rettighetshaveren for å få dekket sitt tap. Det må deretter foreligge et ansvarsgrunnlag, i dette tilfellet culpaansvar, og det må være en adekvat årsakssammenheng mellom tapet og ansvarsgrunnlaget.

Det er ikke uten videre åpenbart at det foreligger adekvat årsakssammenheng ved misbruk av digital signatur. Spørsmålet om adekvat årsakssammenheng ble behandlet i Gjøvik tingrett.[52] I saken hadde en person blitt svindlet av sin samboer gjennom 30 år etter å ha oppgitt sitt passord til vedkommende. Samboeren hadde deretter på utspekulert vis forfalsket lønnsslipper, oppgitt sin egen e-postadresse og et telefonnummer som ikke eksisterte, for å signere låneavtaler. Retten konkluderte med at det forelå årsakssammenheng, men at denne ikke var adekvat ettersom svindelofferets rolle var så lite fremtredende. Det har også blitt løftet en diskusjon om misbruk av BankID for å signere forbrukslån i det hele tatt skal ha erstatningsrettslig vern, spesielt sett hen til adekvansvurderingen.[53] Det vil imidlertid føre for langt for oppgaven å gå i dybden på disse spørsmålene.

Alle tre vilkårene må være oppfylt for at tjenesteyteren som har innvilget og utbetalt et lån skal kunne fremme krav mot rettighetshaveren. Om rettighetshaveren ilegges ansvar, kan ansvarsbegrensningene i annet til femte ledd påberopes. Dette innebærer på den annen side at dersom rettighetshaveren ikke har opptrådt uaktsomt, er vilkåret ikke oppfylt. Følgelig vil

---

50 Hagstrøm (2011) s. 466.

51 Hagstrøm (2011) s. 466.

52 TGJOV-2017-170313.

53 https://rett24.no/articles/bankid-erstatningsrett-pa-ville-veier [hentet 14.5.21].

ikke banken kunne fremme krav, ettersom bestemmelsen ikke kommer til anvendelse, og rettighetshaveren kan heller ikke holdes ansvarlig.

3.4 Rettighetshaverens plikter

Rettighetshaverens ansvar etter finansavtaleloven 2020 § 3-20 fastlegges etter en vurdering i to ledd. For det første må det foreligge brudd på kundens plikter etter § 3-19. Deretter vil omfanget av kundens ansvar bero på hvilken grad av skyld kunden har utvist ved brudd på disse pliktene. Det må derfor gjøres en vurdering av hvilke plikter som eventuelt må brytes for at ansvar skal være aktuelt etter bestemmelsen.

Det følger av § 3-19 første ledd at kunden skal bruke de «elektroniske signaturfremstillingsdataene» i samsvar med «vilkårene for utstedelse og bruk» og skal ta «alle rimelige forholdsregler for å beskytte personlig sikkerhetsinformasjon». Vilkårene for utstedelse og bruk skal være «objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet».

Det er «personlig sikkerhetsinformasjon» rettighetshaveren plikter å beskytte med «alle rimelige forholdsregler». Etter finansavtaleloven 2020 § 1-8 tiende ledd er «personlig sikkerhetsinformasjon» definert som «personaliserte innretninger som en tjenesteyter stiller til rådighet for kunde eller annen bruker for autentiseringsformål». I merknadene til finansavtaleloven 2020 § 3-20 vises det til «signaturfremstillingsdata og sikkerhetsordninger».[54] Med dette siktes det til både eventuell brikke, passord og engangskoder. Det kan likevel også omfatte andre personaliserte innretninger som benyttes for å fremstille signatur, ettersom begrepet er teknologinøytralt.

Ordlyden av «alle rimelige forholdsregler» tilsier at det kreves av rettighetshaveren at iverksetter tiltak for å beskytte den personlige sikkerhetsinformasjonen, men at tiltakene ikke skal hemme bruken – at de er rimelige. Tiltakene som kan kreves må derfor være innenfor rimelighetens grenser. En alvorlig begrensning av bruken vil ikke kunne kreves,

Høyesterett har slått fast at en «rimelig forholdsregel» etter finansavtaleloven 1999 § 34 må «bygge på hva som er praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren

[54] Prop. 92 LS (2019-2020) s. 358.

eller vil gjøre selve bruken av BankID upraktisk».[55] En naturlig forståelse av uttalelsen tilsier at hvilke tiltak som må iverksettes, kan variere, men at det må være både praktisk mulig å gjennomføre, og at tiltakene ikke må være for inngripende i bruken.

Plikten henger tett sammen med vilkårene for utstedelse og bruk, og det kan være vanskelig å skille pliktene, ettersom også vilkårene ofte regulerer beskyttelse av personlig sikkerhetsinformasjon.

Vurderingen av «alle rimelige forholdsregler» er en henvisning til aktsomhetsgrunnlaget som dette må inngå i. Dette er nærmere behandlet i HR-2020-2021-A. Dommen analyseres i kapittel 4.2. Vurderingen vil derfor foretas der.

Aktsomhetsplikten er som utgangspunkt knyttet til forpliktelsene etter vilkårene for utstedelse og bruk. Det er kontraktsfrihet i norsk rett, og det vil kunne eksistere en rekke ulike avtaletekster som kunden kan inngå med ulike tjenestetilbydere for bruk av BankID for sin bestemte tjenesteyter. I praksis er avtalene veldig like hos de fleste utstedere, med små variasjoner. Det er likevel en åpning for at hver enkelt utsteder har sin egen avtale, med særegne avtalevilkår. Rettighetshaverens plikter etter avtalen må utledes konkret i avtaleteksten, med utgangspunkt i avtalens objektive innhold basert på en naturlig språklig forståelse.[56]

At rettighetshaverens plikter etter avtalen også er hjemlet i loven, gjør likevel at disse må sees opp mot de øvrige vilkårene, herunder «alle rimelige forholdsregler» og at vilkårene må være «objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet». Dette innebærer at pliktene må sees i sammenheng. Jeg vil først vurdere pliktene etter den generelle BankID-avtalen.

De generelle vilkårene til BankID er regulert i «Avtalevilkår for PersonBankID og Ansatt-BankID – PDS», sist vedtatt 21. mai 2019.[57] Det kan som nevnt tenkes avtaler med annen ordlyd hos ulike tjenesteytere, men det tas her utgangspunkt i denne generelle avtalen.

---

55 HR-2020-2021-A avsnitt 98.

56 Rt. 1997 s. 1807 på s. 1813.

57 https://www.bankid.no/globalassets/dokumenter/apne-sider/bankid/dnb_pds_personal-v1.1.pdf [Hentet 17.5.21].

Kapittel 4 regulerer kundens ansvar. I punkt 4.1 om vern av passord og sikkerhetsprosedyrer fremgår det at:

> *«BankID er personlig og skal ikke overdras eller på annen måte overlates til eller brukes av andre enn Kunden eller Brukeren. Passord, personlige koder og andre sikkerhetsprosedyrer må ikke røpes for noen, heller ikke overfor politiet, Utsteder eller husstandsmedlemmer. Kunden og Brukeren skal benytte oppdatert programvare, herunder operativsystem, nettleserprogram og annen programvare for sikker kommunikasjon med nettstedet, samt antivirusprogramvare. For øvrig skal Kunden eller Brukeren følge Utsteders til enhver tid gjeldende sikkerhetsråd.»*

Av dette kan det utledes at BankID ikke skal 1) «overdras eller på annen måte overlates» til andre, 2) at passord, personlige koder og andre sikkerhetsprosedyrer ikke må «røpes» for noen, 3) at kunden skal bruke oppdatert programvare, og at kunden skal 4) følge utsteders til enhver tid gjeldende sikkerhetsråd.

En alminnelig språklig forståelse av «overdras» tilsier at det er tale om å varig gi bort selve brikken til andre enn den som har inngått avtalen, altså kunden. At noe ikke skal «overlates», peker mot et mer midlertidig preg som krever en noe mer aktiv handling. At noe overlates til andre, kan også skje ved en passiv handling, altså at brikken legges igjen en annen plass. Samlet sett må plikten derfor sies å være at brikken verken varig eller for en kortere periode settes i andres kontroll.

At passord, personlige koder og andre sikkerhetsprosedyrer ikke må «røpes», peker mot å aktivt gi bort dette til tredjeperson. Å røpe noe krever imidlertid ikke at dette er gjort muntlig. Om passordet skrives ned og gis bort aktivt, eller blir oppdaget, må dette sies å være omfattet av ordlyden. Etter ordlyden settes det et strengt krav til dette, da det ikke må røpes for «noen», heller ikke overfor politiet, utsteder eller husstandsmedlemmer. En naturlig tolkning er derfor at passordet ikke under noen omstendigheter må, verken muntlig eller skriftlig, gis til andre enn rettighetsinnehaveren.

Hva som ligger i at kunden skal følge «[u]tsteders til enhver tid gjeldende sikkerhetsråd», gir ingen konkret anvisning, og må i så fall legge opp til at kunden til enhver tid oppdaterer seg

på nøyaktig hva disse rådene er for å opprettholde plikten. At det er råd som er til «enhver tid gjeldende», tilsier likevel at disse rådene kan endre seg, og at det kan skje ensidig. Det innebærer en plikt til å være oppdatert jevnlig og etterleve disse rådene.

Samlet sett er det svært strenge plikter etter avtalen. Til tross for at kunden etter § 3-19 plikter å følge vilkår for utstedelse og bruk, må dette sees i sammenheng med at disse pliktene også må være «rimelige forholdsregler» og «stå i forhold til formålet».

3.4.1 Hvor langt kan vilkår for utstedelse og bruk strekke seg?

Basert på de strenge pliktene etter avtalen reiser det seg et spørsmål om pliktene kan strekke seg så langt tjenesteyteren måtte ønske sett opp mot at det må være «rimelige forholdsregler» og «stå i forhold til formålet».

Finansavtaleloven kan som nevnt ikke fravikes ved avtale til skade for forbrukeren, jf. § 1-9. Hensikten med loven er å verne om forbrukere og sikre en balansering av maktassymetrien som eksisterer mellom partene. Formålet med avtalen er å regulere partenes plikter. Det er imidlertid svært strenge plikter som går langt i å oppstille krav som for mange vil være vanskelig å oppfylle. Om pliktene medfører så strenge plikter at det i realiteten er tale om et objektivt ansvar, vil det uthule regelverket, og langt raskere medføre at rettighetshaveren havner i ansvar. Det vil i så fall være i strid med formålet til loven.

Det er etter BankID-avtalen strenge regler for å beskytte den personlige sikkerhetsinformasjonen. Dette er imidlertid også regulert i § 3-19, hvor rettighetshaveren skal ta alle «rimelige forholdsregler» for å beskytte denne. Om kontraktsvilkåret skjerper denne plikten, må det sies å både kollidere med hva som er en rimelig forholdsregel, og heller ikke være en plikt som står i forhold til formålet.

Det kan også reises spørsmål ved om det er en «rimelig forholdsregel» å nekte en rettighetshaver å oppgi informasjonen til politiet dersom disse spør om informasjonen. Dette vil potensielt være i strid med lov om politiet 1. oktober 1995 nr. 16 § 5, hvor «[e]nhver plikter straks å rette seg etter de pålegg, tegn eller øvrige signaler politiet gir».

Det er også høyst usikkert hvordan brudd på «enhver tid gjeldende sikkerhetsråd» skal vurderes, og hvilket tidspunkt banken kan gjøre det gjeldende at rådet gjelder.

I tillegg kommer at vilkårene for utstedelse og bruk i stor grad må anses som standardavtaler, hvor rettighetshaveren ikke har innvirkning på utformingen av avtalen. Valget står da mellom å akseptere vilkårene eller være avskåret fra å ta i bruk BankID. Når rettighetshaveren da er forpliktet til å følge «enhver tid gjeldende sikkerhetsråd» vil tjenesteyteren ensidig kunne endre vilkårene. EUs direktiv om urimelige kontraktsvilkår i forbrukeravtaler (direktiv 1993/13) er en del av EØS-avtalen, og regulerer avtaler mellom forbruker og næringsdrivende. Norske domstoler må se hen til direktivet, og gi forbrukerne det vernet direktivet påbyr.[58]

I direktivet finnes den såkalte grålisten som er inntatt i bilaget i slutten av direktivet. I listens bokstav i heter det at «Kontraktvilkaar, hvis formaal eller virkning er foelgende: i) bindende for forbrugeren at fastslaa, at denne har accepteret vilkaar, som han rent faktisk ikke har haft mulighed for at stifte bekendtskab med inden aftalens indgaaelse». Det synes klart at en ensidig endring av vilkårene vanskelig vil kunne være i tråd med dette. Det kan derfor stilles spørsmålstegn ved om en slik plikt vil kunne påberopes av tjenesteyteren som grunnlag for ansvar.

Det er etter dette uklart hvor langt pliktene i vilkår for utstedelse og bruk kan strekke seg. En tolkning av § 3-19 første ledd kan tilsi at de strenge kravene i vilkårene er like bindende. Det vil innebære at ulike kunder som benytter samme tjeneste, men med ulike tilbydere, har ulike rettigheter. En alternativ tolkning er at vilkårene tolkes innskrenkende slik at vilkårene sensureres dersom disse utgjøre en urimelig forholdsregel. Selve bestemmelsen gir ikke veiledning for utfallet.

Det må da vektlegges at finansavtaleloven er ufravikelig til skade for forbruker. For strenge vilkår må sies å være en avtale som er til skade for forbrukeren. Om vilkårene er bindende fullt ut, vil dette i praksis medføre at det er utsteder som setter grensene for den utviste skyld, og dermed innfører vilkår i strid med tersklene lovgiver har valgt i § 3-20. Det vil stride mot lovens system og hensynene bak.

[58] Giertsen (2014) s. 206.

Etter dette må det legges til grunn at vilkårene ikke kan innebære plikter som ikke utgjør en «rimelig forholdsregel», og heller ikke så strenge plikter at det strider mot formålet.

4 Når har rettighetshaveren handlet uaktsomt?

4.1 Innledende om uaktsomhetsvurderingen

Etter finansavtaleloven 2020 § 3-20 første ledd kan tjenesteyteren gjøre gjeldende erstatningsansvar gjeldende i samsvar med «ellers gjeldende rettsregler». For hva som ligger i «ellers gjeldende rettsregler», vises det til kap. 2.2.3. Kjernen i dette er ansvar etter den alminnelige culparegelen, og alminnelig uaktsomhet er inngangsvilkåret.

Spørsmålet som skal besvares i dette kapittelet, er hva som regnes som erstatningsbetingende uaktsom atferd av en rettighetshaver for en BankID-brikke.

I forarbeidene er det uttalelser som kan gi veiledning til aktsomhetsvurderingen etter alminnelig erstatningsrett. For det første pekes det på at i tilfeller hvor tredjepart uberettiget tilegner seg signaturfremstillingsdata, vil ansvaret bero på en «konkret vurdering».[59] Ordlyden tilsier at det som utgangspunkt skal gjøres en helhetsvurdering av rettighetshaverens handlemåte i vurderingen av ansvaret. Dette tilsier at alle ulike faktorer som spiller inn i den aktuelle situasjonen, må tas i betraktning.

Videre er det pekt på konkrete tilfeller som anses uaktsomme.[60] Det vil eksempelvis være uaktsomt å «skrive ned passord eller koder på en slik måte at de enkelt vil kunne misbrukes av tredjepart». [61] Uttalelsen må tolkes dithen at det ikke anses uaktsomt i seg selv å skrive ned passord eller koder. Dersom dette gjøres på en måte som gjør det «enkelt» for tredjeperson å misbruke den digitale signaturen stiller dette seg annerledes. Det er ingen holdepunkter for hva som er «enkelt», men det kan peke mot både hvor nedskrivingen er gjort, eksempelvis i et notat på mobilen eller på en fysisk lapp, og om denne oppbevares i nærheten av BankID-brikken. At noe er «enkelt» tilsier at det må være gjort på en måte hvor svindler uten større komplikasjoner kan gjennomføre svindelen. Dette tilsier også at det skal noe mer til å konkludere med erstatningsbetingende uaktsomhet dersom svindleren går mer systematisk til verks.

---

59 Prop. 92 LS (2019-2020) s. 358.

60 Prop. 92 LS (2019-2020) s. 358.

61 Prop. 92 LS (2019-2020) s. 358.

At noe er «enkelt» kan også peke på at dersom passord nedskrives bør det ikke være enkelt å forstå hva nedskrivingen knytter seg til, eksempelvis gjennom å skrive «Kode til BankID-brikke». Det kan av forarbeidenes ordlyd ikke utledes et krav til å skrive ned passordet kamuflert i koder eller lignende, men at rettighetshaveren lettere kommer i ansvar i disse tilfeller.

Dette er også et praktisk eksempel. I en digital hverdag hvor det kreves passord på stadig flere plattformer, vil det for mange være nødvendig å på en eller annen måte notere ned koder for å holde styr på innloggingsinformasjonen. Dette tilsier at nedtegning av passordet ikke alene er uaktsomt, og ikke i seg selv kan medføre ansvar. Det må likevel gjøres en helhetlig vurdering av situasjonen, i tråd med at det skal foretas en «konkret vurdering».

Videre trekkes det frem tilfeller hvor tredjeparten benytter seg av «avanserte metoder» for å fremskaffe passord og koder, herunder skjult filming, overvåking av mobiltelefon og datamaskiner o.l. For en uvitende person vil det være «nærmest umulig» å beskytte seg mot dette, og trekkes frem som tilfeller hvor det «skal mye til» for å konstatere uaktsomhet. [62] Dette henger også tett sammen med at det i slike tilfeller vil være svært få handlingsalternativer for rettighetshaveren, jf. ordlyden «nærmest umulig». Det vil da være vanskelig å klandre rettighetshaveren for handlemåten, men det utelukkes ikke. Det tilsier at uaktsomhet ikke er utelukket i disse tilfellene, men at terskelen settes relativt høyt før ansvar kan være aktuelt.[63]

Et siste eksempel som trekkes frem, er at det ikke er uaktsomt i seg selv av «familiemedlemmer å dele postkasse» slik at andre i familien potensielt får uberettiget tilgang til rettighetshaverens post.[64] Dette tilsier at dersom den uvedkommende tredjeparten skaffer seg tilgang gjennom å urettmessig åpne posten, vil det ikke kunne konstateres ansvar basert på dette alene. At det konkret pekes mot familiemedlemmer, tilsier også at tilfeller hvor uvedkommende har stjålet posten vil dette heller ikke kunne anses uaktsomt – det ville innebåret at det å motta post i seg selv kan medføre ansvar.

---

62 Prop. 92 LS (2019-2020) s. 358.

63 Prop. 92 LS (2019-2020) s. 358.

64 Prop. 92 LS (2019-2020) s. 358.

Høyesterett har i HR-2020-2021-A tatt stilling til kundens ansvar i et svindeltilfelle hvor hans digitale signatur ble misbrukt. Dommen er sentral fordi det hittil er den eneste som vurderer aktsomhetsterskelen ved misbruk av digital signatur. Selv om saken handler om et spesifikt typetilfelle, kommer Høyesterett med uttalelser som gir retningslinjer som er relevant for vurderingen av når en rettighetshaver har opptrådt uaktsomt.

4.2 HR-2020-2021-A

Saken gjaldt en person (A) som hadde fått sin BankID misbrukt av ekteparet B og C. Ekteparet hadde inngått flere lån i As navn, og var straffedømt for forholdene da saken kom opp for Høyesterett. Spørsmålet for Høyesterett var om A hadde opptrådt erstatningsbetingende uaktsomt, slik at EasyBank, som hadde utbetalt et forbrukslån etter misbruket av BankID-brikken, kunne kreve tapet erstattet av A. Høyesterett konkluderte med at det ikke forelå ansvarsgrunnlag. A kunne følgelig ikke holdes ansvarlig for EasyBanks tap. Avgjørelsen var enstemmig.

Dommen ble avsagt før den nye finansavtaleloven har trådt i kraft. Høyesterett kom i dommen med flere avklaringer som vil være retningsgivende for fremtidige saker, og vil fortsatt ha relevans i fremtiden, ettersom ansvarsgrunnlag etter alminnelig erstatningsrett er inngangsvilkåret for at ansvar skal være aktuelt etter finansavtaleloven 2020 § 3-20 første ledd.

I det følgende vil jeg fokusere på uaktsomhetsvurderingen som foretas i dommen, hvilke vurderingstema Høyesterett bruker og prejudikatsrekkevidden for lignende svindeltilfeller.

4.2.1 Sakens faktum

A drev flere gatekjøkken i Sørlandsområdet, og kjente i forkant av misbruket C. A hadde BankID-avtale hos DNB og konto tilknyttet minst to banker. As BankID-brikke ble oppbevart på et av gatekjøkkenene, liggende på en kontorplass i en veske plassert i en skuff med andre kodebrikker. Kontorplassen var ikke adskilt fra de øvrige lokalene. Skuffen var ikke sikret med lås og var følgelig tilgjengelig for andre ansatte som hadde tilgang til dette området.

I tidsperioden 15. februar til 10. mars 2017 ble As BankID misbrukt en rekke ganger til å signere flere låneopptak hos ulike finansinstitusjoner. Lånet som var til behandling for Høyesterett, var et forbrukslån hos EasyBank på kroner 100 995. I det aktuelle tidsrommet hvor låneopptaket fant sted var A på ferie, og retten la til grunn at C én eller flere ganger hadde tatt med seg brikken bort fra kontorplassen for å gjennomføre svindlene.

For å benytte BankID som elektronisk signatur var det imidlertid ikke nok å ha tilgang til brikken; ekteparet måtte også ha kjennskap til As personlige passord. I saken var det uklart hvordan de hadde fått kjennskap til dette, men det ble påpekt at As postkasse våren 2017 ble brutt opp og at uåpnet post tilhørende A ble funnet hjemme hos ekteparet B/C.

4.2.2 Forhold på skadevolders side

Det var to forhold som fra bankens side var påberopt å utgjøre erstatningsbetingende uaktsom opptreden: «oppbevaringen eller behandlingen av passordet» og «oppbevaringen av kodebrikken».[65]

EasyBank anførte at A hadde opptrådt uaktsomt i sin behandling av passordet. Ingen av partene visste hvordan ekteparet som hadde gjennomført misbruket, fikk tak i passordet. Dermed kunne ikke EasyBank sannsynliggjøre at det forelå uaktsomhet ved behandlingen av passordet.

Høyesterett uttaler seg ikke generelt om hva som er en kundes plikter i forbindelse med hvordan passordet håndteres. Når det likevel tas opp som en problemstilling, tilsier dette i seg selv at Høyesterett åpner for at en kundes håndtering passordet kan medføre ansvar. Sett hen til uttalelsene i forarbeidene om nedtegning av passord tilsier dette at ansvar kan forekomme, men at det da må noe mer til enn nedtegning i seg selv. Systembetraktninger tilsier også at dette kan være tilfellet ettersom uvedkommende ikke vil kunne gjennomføre svindelen uten å få tilgang til passordet. Dette er også en plikt som kan utledes av finansavtaleloven 2020 § 3-19, som etter loven vil være gjenstand for vurdering.

Ettersom det ene alternativet – uforsiktig håndtering av passord – ikke førte frem, var det As oppbevaring av kodebrikken som ble det sentrale for vurderingen av om A hadde opptrådt erstatningsbetingende uaktsomt.

Det sentrale vurderingstemaet var om A hadde tatt «alle rimelige forholdsregler» for å verne seg mot misbruk av BankID-brikken.[66] Normen er lovfestet i finansavtaleloven 1999 § 34,

---

65 HR-2020-2021 avsnitt 95.

66 HR-2020-2021-A avsnitt 54.

som i stor grad samsvarer med den nye lovens § 3-19. Høyesterett slår fast at normen gjelder også utenfor lovens virkeområde. Dette innebærer at alle innehavere av BankID vil måtte ta «alle rimelige forholdsregler» for å verne seg, uavhengig av hvilken avtale som er inngått og hvor denne gjelder. Det er altså tale om en alminnelig norm som alle innehavere vil kunne vurderes etter på dette livsområdet.

Høyesterett presiserer at innholdet i normen må «bygge på hva som [er] praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren eller vil gjøre selve bruken av BankID upraktisk.»[67] Dette må forstås som at en innehaver har plikt til å iverksette tiltak for å beskytte seg mot misbruk, men ikke i en slik grad at det ikke lenger er praktisk mulig å benytte seg av brikken til sitt tiltenkte formål. BankID er for de fleste blitt en nødvendighet i hverdagen, og en rekke både offentlige og private tjenester krever innlogging ved bruk av BankID som identifikasjon. Hva som regnes som uaktsomt må følgelig ta denne bruken med i vurderingen, og sees i lys av hvordan bruken normalt skjer.[68] Det kan av uttalelsen ikke utledes hva som er en «urimelig stor byrde», men det tilsier at det både må gjøres en konkret vurdering av det aktuelle tiltaket, om dette kan anses som en «byrde» og deretter om denne byrden er «urimelig». En byrde som ikke er rimelig, vil dermed være i strid med normen.

Høyesterett uttaler deretter at det ikke vil være uaktsomt å oppbevare brikken hjemme, selv ikke om brikken ligger åpent og tilgjengelig. Det slås deretter fast at det «bare i særlige tilfeller [vil] være aktuelt å anse en oppbevaring hjemme som uaktsom.»[69]

Av dette kan det utledes at oppbevaring av BankID-brikke i hjemmet svært sjelden vil medføre uaktsomhet, jf. «særlige tilfeller». Dette underbygges i samme avsnitt med at en bolig er låst og normalt ikke tilgjengelig for andre enn husstandsmedlemmene og deres gjester. Dette synes å peke mot skaderisikoen, som må antas å være lav i hjemmet. Det kan likevel ikke tolkes dithen at uaktsomhet er utelukket i alle tilfeller hvor brikken er oppbevart hjemme. Men en slik oppbevaring vil som den klare hovedregel ikke medføre ansvarsbetingende uaktsomhet. Det presiseres ikke hva som er «særlige tilfeller». Ordlyden tilsier at det må være tilfeller utover det vanlige, eksempelvis i en konkret situasjon hvor rettighetshaveren vet at risikoen

---

67 HR-2020-2021-A avsnitt 98.

68 HR-2020-2021-A avsnitt 98.

69 HR-2020-2021-A avsnitt 99.

for svindel er tilstede, eksempelvis ved at en i husstanden eller noen i omgangskretsen har misbrukt rettighetshaverens BankID-brikke tidligere. Uttalelsen tilsier likevel at det selv i disse tilfeller skal mye til før rettighetshaveren kan holdes ansvarlig. I motsatt fall ville det kunne bidratt til en generell mistenkeliggjøring mellom nærstående på generelt grunnlag, noe som ikke kan sies å være formålstjenlig. Et krav om nedlåsning eller lignende ville også harmonert dårlig som en «rimelig forholdsregel», da dette ville blitt urimelig byrdefullt. Det må bemerkes at det her er tale om oppbevaring av brikken alene – ikke tilfeller hvor brikke og passord oppbevares samlet.

For oppbevaring på arbeidsplassen uttaler Høyesterett at det «i større grad må foretas en konkret vurdering».[70] Ikke «enhver oppbevaring» som «skaper mulighet for at andre kan ha tilgang til brikken» kan regnes som uforsvarlig, og dermed medføre erstatningsbetingende uaktsomhet. Konkret vises det videre til at det *ikke* kan kreves at brikken skal låses ned hver gang innehaveren forlater arbeidsplassen, men at det kreves en «viss kontroll» på brikken.[71]

Dette viser at det kreves en større grad av sikring fra innehaveren så raskt brikken oppbevares utenfor hjemmet. Dette på bakgrunn av den usikkerhet slik oppbevaring gir både knyttet til hvilke personer som kan få tilgang til brikken i tillegg til kontroll og oversikt over hvem dette kan være. I et næringslokale med gjester og ansatte vil det av naturlige årsaker oppholde seg en videre krets av ukjente personer, gjerne opptil flere hver eneste dag. Kravene til innehaveren skjerpes derfor i slike tilfeller, slik at det skal mindre til for å konstatere uaktsomhet sammenlignet med tilsvarende oppbevaring i hjemmet. At det ikke kan kreves at brikken låses ned viser imidlertid at det er en yttergrense for hvor strenge tiltak en innehaver kan avkreves. Det kan eksempelvis ikke uten videre kreves at innehaveren går til innkjøp av safe eller andre låsbare objekter for å verne om brikken.

I den konkrete vurderingen av As oppbevaring av brikken legges det til grunn at brikken var «plassert i en veske som var plassert i en skuff i et skap», og dermed ikke har ligget «fritt og tilgjengelig». Dette tilsier at om brikken hadde ligget oppe i dagen, lett synlig og tilgjengelig, vil ikke dette være tilstrekkelig sikring, ettersom kontorplassen som sådan var tilgjengelig for

[70] HR-2020-2021-A avsnitt 100.

[71] HR-2020-2021-A avsnitt 101.

andre.[72] Det sentrale blir i så måte om brikken på en eller annen måte er forsøkt skjult og gjort utilgjengelig for uvedkommende, og hvor godt dette er gjort. I det aktuelle tilfellet var oppbevaringen av BankID-brikken ikke uforsvarlig. Uttalelsen kan likevel ikke tolkes som et absolutt krav om å legge brikken i en veske i en skuff i et skap – også enklere oppbevaring må kunne aksepteres uten at det i seg selv medfører erstatningsbetingende uaktsomhet. Uttalelsen åpner også for et annet utfall dersom kontorplassen ikke er tilgjengelig for alle ansatte – det er kretsen av personer som potensielt får tilgang som synes å være det avgjørende. Det vil avhenge av en helhetsvurdering av hvem som har tilgang til oppbevaringsplassen og hvor enkelt det er å finne brikken.

Høyesterett peker også på at brikken har vært oppbevart på denne måten i en «lang periode», også mens A var på ferie. I tidsrommet A var på ferie uttales det videre at BankID-brikken burde vært «nedlåst, eller han burde tatt den med seg».

Tidsaspektet får dermed vekt. Jo lengre en brikke blir liggende tilgjengelig på denne måten, jo større blir muligheten for misbruk. Uttalelsen kan heller ikke her tolkes som et absolutt krav til at brikken låses ned eller tas med hjem, men at det skjerper kravet til aktsomhet. I dette ligger også en risikobetraktning; skaderisikoen øker jo lengre brikken blir liggende uten tilsyn uten at rettighetshaveren har kontroll på den. Høyesterett uttaler at A kan «bebreides for den måten han oppbevarte kodebrikken på», men konkluderer likevel med at handlemåten ikke medfører ansvarsbetingende uaktsomhet. Dette gjøres etter en helhetsvurdering, noe som er i tråd med hva som kan utledes av forarbeidene, hvor det nettopp legges opp til en «konkret vurdering».

Alt dette var forhold på kundens side. Høyesterett kommer imidlertid med uttalelser om forhold på skadelidtes side, som er avgjørende for hvilke handlinger som medfører erstatningsbetingende uaktsomhet.

4.2.3 Forhold på skadelidtes side

Høyesterett kommer med prinsipielle uttalelser om forhold på skadelidtes side, som har stor vekt ved vurderingen av om kunden har opptrådt erstatningsbetingende uaktsomt.

---

[72] HR-2020-2021-A avsnitt 102.

Når uaktsomhet skal vurderes, og terskelen settes, uttales det i avsnitt 61 at:

> *Der avtaleparten, tjenesteyteren, tilhører en gruppe som kan forventes selv å iverksette tiltak for å unngå tap, må dette etter mitt syn få betydning når man skal stilling til om innehaveren i det enkelte tilfellet har opptrådt uaktsomt og ut fra det blir erstatningsansvarlig.*

Det legges til grunn at culpanormen som utgangspunkt er objektiv, og at erstatningsansvar kan pålegges den enkelte som «kunne og burde handlet annerledes», men at det «likevel [er] rom for en viss relativisering»,[73] og at en og samme handling kan vurderes som uaktsom i relasjon til en gruppe skadelidt, i dette tilfellet banken, sammenlignet med en annen gruppe skadelidte. Sentralt her er rolleforventningen til skadelidte. Konkret pekes det på at det i enkelte tilfeller vil være åpning for at ansvaret faller bort dersom skadelidte står nærmest til å foreta tiltak som kan eliminere risikoen.

I denne undergruppen har skadelidte risikoen for skaden som oppstår. Skadelidte, i dette tilfellet EasyBank, skal gjøre sitt for at risikoen for tap blir så liten som mulig. I slike tilfeller må skadelidte tåle både risiko og skade, og skadevolder må følgelig frifinnes.[74]

Her tegner Høyesterett opp et sentralt skille mellom krav til banken for ikke godkjente betalingstransaksjoner og tilfeller hvor BankID brukes for å signere en avtale frem. I førstnevnte tilfeller kan det ikke forventes at banken iverksetter sikringstiltak, fordi iverksettelse av betalingsordre hos en allerede eksisterende kunde er en alminnelig handling som i utgangspunktet ikke bør vekke mistanke hos banken uten videre. I sistnevnte tilfelle er det tale om en avtale med «vidtrekkende økonomiske konsekvenser for innehaveren med en bank som han ikke hadde noe kundeforhold til.»[75]

Uttalelsen er et obiter dictum, og det kan stilles spørsmålstegn ved om standpunktet kan opprettholdes. En slik forskjellsbehandling trekker opp et kunstig skille mellom de to situasjone-

---

73 HR-2020-2021-A avsnitt 56.

74 HR-2020-2021-A avsnitt 57.

75 HR-2020-2021-A avsnitt 59.

ne. I tillegg kommer at bankene er ilagt omfattende plikter for overvåkning også av betalingstransaksjoner for å avdekke svindel, samt å avdekke hvitvasking og terrorfinansiering.[76] Det som imidlertid kan trekkes ut, er at skadelidtes mulighet til å avverge risikoen *skal* tillegges vekt ved inngåelse av kredittavtale.

En slik risikobetraktning som Høyesterett foretar her, er noe annet enn en reduksjon av erstatningsansvaret som følge av skadelidtes medvirkning etter skadeserstatningsloven § 5-1. En vurdering av medvirkning er først aktuelt etter at ansvar er konstatert hos skadelidte. Det sentrale i et tilfelle som dette, er hvem som har «skapt risikoen og hvem som er nærmest til å iverksette tiltak for å unngå tap».[77] Det må dermed ved fastsettelse av uaktsomhetsterskelen gjøres en vurdering av hvor fremtredende skadevolders rolle er i at skaden oppstår, sett opp mot hvilke tiltak skadelidte kan iverksette for å minimere skaderisikoen. Jo enklere tiltak skadelidte kan iverksette, jo mer fremtredende blir skadelidtes rolle, noe som påvirker om skadevolder har opptrådt uaktsomt og hvor terskelen settes.

I Høyesterett ble det først vurdert hvordan A hadde oppbevart brikken. Som tidligere nevnt var den plassert i en veske, i en skuff inne i et skap. Den lå også plassert her i en lengre tidsperiode mens A var på ferie. Selv om A kunne «bebreides» for oppbevaringen, var det forholdene på EasyBanks side som var avgjørende for konklusjonen.

At EasyBank er en «profesjonell aktør», men likevel har valgt å inngå avtale om et lånebeløp som for en enkeltperson er «betydelig», og at innvilgelsen har skjedd «utelukkende basert på identifikasjon og elektronisk signatur gjennom BankID», fikk avgjørende vekt.[78] Det pekes på at det var mulig for banken å «foreta ytterligere kontrolltiltak» før utbetalingen fant sted. Med slike enkle tiltak, som eksempelvis å ringe kunden, sjekke om kontoen står i låntakers navn eller sendt en SMS, var det «stor sannsynlighet for at misbruket ville vært unngått». Banken har da «bevisst valgt en handlemåte som innebar en klar risiko for tap».[79]

---

76 Se Lov 1. juni 2018 om tiltak mot hvitvasking og terrorfinansiering.

77 Kjørven (2020).

78 HR-2020-2021-A avsnitt 104.

79 HR-2020-2021-A avsnitt 104.

Høyesterett peker her på at det er banken som med enkle tiltak kunne innrettet seg på en måte som hadde nærmest fjernet risikoen. Dette er i kjernen av de risikobetraktninger som det ble pekt på tidligere. Selv om A hadde opptrådt «noe uforsiktig»,[80] var det bankens handlemåte som var fremtredende for at risikoen ble realisert. Når terskelen skal settes er det dermed sentralt å vurdere hvilke tiltak skadelidte har i sin verktøykasse og hvor enkelt det er å iverksette disse.

Dette peker mot en mer generell vurdering i saker som den foreliggende. For banker er det relativt enkle tiltak som kan gjennomføres for å sikre at den som signerer lånet digitalt rent faktisk er personen som har søkt om det. Høyesterett nevner tiltak som å sjekke at kontoen lånet utbetales til står i låntakers navn. Det kan imidlertid tenkes flere tiltak, og at Høyesterett er åpen for dette, jf. uttalelsen «ett av tiltakene som en utlånsbank bør benytte».[81] Det kan da tenkes flere tiltak, som eksempelvis en SMS til vedkommendes registrerte telefonnummer eller en videosamtale med kunden før større summer utbetales. At banken «bør» benytte slike tiltak betyr ikke nødvendigvis at dette er en plikt, men at det er noe som likevel kan forventes – spesielt sett opp mot hvor enkelt det er å undersøke dette. Når det forventes, men ikke gjennomføres, vil det da være urimelig å ilegge rettighetshaveren ansvar. Det harmonerer også godt med pulveriseringshensynet.

Holdt opp mot at BankID-innehavere «generelt må forventes å være klare over risikoen for misbruk», legger Høyesterett videre til grunn at det «fremstår ikke på samme måte som nærliggende at BankID skal kunne benyttes som eneste grunnlag for inngåelse av avtaler i innehavers navn som medfører ansvar for meget høye pengebeløp».[82] Dette er en henvisning til risikoens synbarhet. At det er en teoretisk mulighet for misbruk, er dermed ikke tilstrekkelig til at en normal forbruker kan regne med at et slikt misbruk oppstår utelukkende ved en «noe uforsiktig» behandling av brikken. Dette vil også spille inn på kravene til sikring. Til tross for at det er potensiale for store tap, vil ansvar ikke kunne ilegge nærmest automatisk dersom det ikke er iverksatt strenge sikringstiltak.

---

80 HR-2020-2021-A avsnitt 105.

81 HR-2020-2021-A avsnitt 107.

82 HR-2020-2021-A avsnitt 106.

Dette taler for at forholdene må sees i sammenheng; har banken gjort lite for å minimere risikoen, skal det mer til før kunden blir ilagt ansvar. En slik vurdering vil likevel kunne tenkes å spille inn på grensedragningen mellom simpel og grov uaktsomhet.

Det som likevel blir stående ubesvart med dommen, er hvordan saken ville blitt stilt dersom banken hadde iverksatt tiltakene som Høyesterett trekker frem, og lånet likevel hadde blitt utbetalt. I den helhetsvurderingen som Høyesterett foretar, var As oppbevaring av brikken «noe uforsiktig», men likevel «så begrenset» at det ikke var grunnlag for å konstatere erstatningsansvar. Høyesterett synes her å åpne opp for at terskelen settes annerledes dersom tiltakene som foreslås hadde blitt iverksatt, men lånet likevel hadde blitt utbetalt. I så tilfelle ville muligens oppbevaringen kunne blitt vurdert som så fremtredende at ansvar kunne vært aktuelt.

På den annen side ville dette krevd ytterligere avansert svindelmetode(r) fra svindler(e), på en slik måte at oppbevaringen i seg selv likevel kunne blitt vurdert som lite fremtredende, jf. også uttalelsene i forarbeidene om «avanserte svindelmetoder». Høyesterett lar det imidlertid bli stående ubesvart.

5 Når har rettighetshaveren handlet grovt uaktsomt?

5.1 Innledende om grov uaktsomhet

Etter finansavtaleloven 2020 § 3-20 tredje ledd svarer rettighetshaveren med en egenandel på inntil 12 000 kroner dersom tapet skyldes at vedkommende «grovt uaktsomt» har unnlatt å oppfylle sine plikter etter § 3-19 første og annet ledd.

En naturlig forståelse av «grov uaktsomhet» tilsier at det er en høy terskel og at det er de mer alvorlige tilfellene av handlinger rettighetshaveren kan bebreides for som rammes.

I merknadene til bestemmelsen er det ikke gitt særskilte vurderinger av hva som anses grovt uaktsomt. Det er imidlertid uttalt at det er uaktsomt å skrive ned passord og koder slik at de «enkelt» vil kunne misbrukes av tredjepart. I tilfeller hvor svindler har benyttet avanserte metoder, herunder skjult filming og overvåking av mobiltelefon og datamaskin, skal det mye til

for å konstatere uaktsomhet.[83] I alle tilfeller skal det foretas en «konkret vurdering» for å vurdere ansvaret. Dersom det er uaktsomt å skrive ned passordet slik at det «enkelt» kan misbrukes av tredjepart, tilsier det at det skal betydelig mer til for at nedtegning skal anses grovt uaktsomt.

I PSD 2 uttales det om «ikke godkjente betalingstransaksjoner» at den grovt uaktsomme atferden må innebære en «vesentlig grad av skjødesløshet», sammenlignet med den alminnelig uaktsomme atferden.[84] Videre uttales det at sikkerhetsopplysningene som brukes for å iverksette og godkjenne transaksjonen, er «oppbevart sammen med betalingsinstrumentet i et format som er åpent og lett gjenkjennelig for tredjemann».[85] Også her «bør det tas hensyn til alle omstendigheter».[86]

At det kreves «vesentlig grad» av skjødesløshet, tilsier at skjødesløsheten må være betydelig. Det kan videre utledes et krav om å ikke oppbevare brikke og et nedtegnet passord samlet dersom nedtegningen er åpenbar eller kamuflert på en måte som lett kan gjennomskues. Om det er oppbevart samlet vil en da raskt ha handlet grovt uaktsomt. Dette kan ikke tolkes som et forbud mot nedtegning, som i seg selv ikke er uaktsomt. Det stilles imidlertid krav til at det ikke oppbevares «åpent» og «lett gjenkjennelig», og i alle tilfeller ikke samlet. Dette tilsier videre at dersom koden er nedskrevet, må dokumentet forsøkes skjult, og at det nedskrevne heller ikke kan være lett gjenkjennelig – et krav om at det forsøkes å kamufleres.

Dette er vurdert i Rt. 2004 s. 499, men med en annen ordlyd i loven og uten dagens direktiver, som jeg vil komme tilbake til under.

I forarbeidene til finansavtaleloven 1999 uttales det at det kreves et «markert avvik fra vanlig forsvarlig handlemåte» for at en handling eller unnlatelse skal kunne karakteriseres som grovt uaktsom.[87] Til tross for at uttalelsene ikke knytter seg til den nye loven, har dette relevans for fastleggelsen av terskelen også i ny lov. Det er heller ikke uttalt i forarbeidene til finansavtaleloven 2020 at en ønsker å gå bort fra denne linjen.

---

83 Prop. 92 LS (2019-2020) s. 358.

84 Direktiv 2015/236/EF fortalens punkt 72.

85 Direktiv 2015/236/EF fortalens punkt 72.

86 Direktiv 2015/236/EF fortalens punkt 72.

87 Se Ot.prp. nr. 94 (2008-2009) s. 117 og NOU 1994:19 s. 144.

Denne tolkningen samsvarer med forståelsen lagt til grunn i Rt. 1989 s. 1318. Høyesterett legger til grunn at for å konstatere grov uaktsomhet må det være tale om en «opptreden som er sterkt klanderverdig, hvor vedkommende altså er vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet».[88] Overført til våre tilfeller må det med da være tale om en konkret vurdering av hvor klanderverdig handlemåten er, og i hvor stor grad rettighetshaveren kan klandres for å ha brutt sine plikter. Dette synes også å samsvare med uttalelsen i fortalen om at det må være tale om en «vesentlig grad av skjødesløshet».[89]

Det sentrale blir da å vurdere i hvilken grad rettighetshaveren er å klandre for å ha mislyktes i å beskytte sin personlige sikkerhetsinformasjon. Det vil være en glideskala fra den alminnelige uaktsomhet og over til de mer skjødesløse handlingene hvor rettighetshaverens unnlatelse er «vesentlig».

Om rettighetshaveren kan klandres, avhenger av om vedkommende «kunne og skulle ha handlet annerledes enn han har gjort».[90] Om handlingen kan karakteriseres som «grovt uaktsom», vil da avhenge av om det er et vesentlig avvik mellom hvordan rettighetshaveren har opptrådt og hvordan vedkommende burde opptrådt.

I vurderingen skal det som utgangspunkt foretas en objektiv vurdering, og det er «ikke en moralsk dom som skal felles».[91]

Det foreligger kun én dom hvor grov uaktsomhet er vurdert etter reglene i finansavtaleloven 1999, slik denne lød før gjennomføring av PSD 1. Til tross for at avgjørelsen knytter seg til en eldre lov, har den likevel relevans, ettersom det også den gang måtte gjøres en vurdering av grensedragningen mellom simpel og grov uaktsomhet. Dommen vil derfor vurderes særskilt i det følgende, med hovedvekt på vurderingstemaer som er relevant for fastleggelsen av hvor terskelen for grov uaktsomhet ligger.

---

88 Rt. 1989 s. 1318 på s. 1322.

89 Direktiv 2015/236/EF fortalens punkt 72.

90 Hagstrøm (2011) s. 468.

91 Hagstrøm (2011) s. 468.

5.2 Rt. 2004 s. 499

Spørsmålet for Høyesterett var om A hadde opptrådt grovt uaktsomt ved å oppbevare sine bankkort sammen med en syvendesans hvor han hadde notert kodene kamuflert. Ett av de stjålne kortene ble benyttet til å ta ut kr. 10.000. Dommen ble avsagt under dissens 3-2, hvor flertallet konkluderte med at A ikke hadde opptrådt grovt uaktsomt.

A var på ferie i Barcelona. Han bodde i en privat leilighet. På avreisedagen var det aktuelle kortet og syvendesansen låst ned i en koffert i leiligheten, som igjen ble nedlåst med både nøkkel og hengelås for noen timer mens A var ute. I perioden A var ute, hadde en eller flere gjerningspersoner brutt seg inn i leiligheten og stjålet blant annet As PC og det aktuelle kortet sammen med syvendesansen. A varslet banken uten ugrunnet opphold og fikk sperret kortene. Før kortene ble sperret, hadde innbruddstyvene gjort uttak på til sammen kr. 10.010 fordelt på seks uttak. Tyvene klarte allerede på fjerde forsøk å gjette seg frem til riktig kode.

Innledningsvis bemerkes det at det i saken var tale om bankkort, og ikke BankID, som er det som skal vurderes i oppgaven. Tilfellene skiller seg fra hverandre ved at det for bankkort kreves kode og kort for å gjennomføre misbruk. For BankID kreves både brikke, passord og personnummer. Det må også påpekes at ordlyden i § 35 i 2004 regulerte kortmisbruk særskilt, og er endret gjentatte ganger siden. Kjernen var likevel, da som nå, den grove uaktsomheten.

DNB anførte to ulike forhold som grovt uaktsomme, og som i kombinasjon ble vurdert av Høyesterett: nedtegningen av koden og oppbevaringen av kort og kode da disse kom på urette hender.[92]

Høyesterett slår fast at grov uaktsomhet fordrer en «kvalifisert form for uaktsomhet». Det påpekes deretter at oppførselen må representere et «markert avvik fra vanlig forsvarlig handlemåte» og at det må dreie seg om «en opptreden som er sterkt klanderverdig» hvor vedkommende er «vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet».[93]

Av dette kan det utledes at uaktsomheten må være kvalifisert, noe som tilsier at det skal mye til. At det kreves et «markert avvik» fra den «vanlig forstandige handlemåte», må forstås som

---

92 Rt. 2004 s. 499 avsnitt 27.

93 Rt. 2004 s. 499 avsnitt 32 med henvisning til Rt. 1989 s. 1318.

at avviket må skille seg klart fra hvordan en alminnelig aktsom person ville opptrådt. Når en slik handlemåte er tilfelle, må skadevolder være «vesentlig mer å klandre». At noen er «vesentlig» mer å klandre, tilsier at handlingen må ha vært svært framtredende i hendelsesforløpet. Følgelig settes terskelen høyt for den grovt uaktsomme atferden. En slik forståelse harmonerer også med forståelsen av alminnelig uaktsomhet i HR-2020-2021-A. Det skal derfor mer til, og terskelen er høy.

For å stille opp en handlingsnorm går Høyesterett først inn i avtalevilkårene for bankkortet. Her fremgikk det at «Pin-koden må ikke noteres». I et skriv A fikk tilsendt sammen med kortet, fremgikk det at «[k]oden må ikke noteres i noen form slik at andre kan finne ut hva tallene gjelder». Disse to uttalelsene, som var en del av As plikter etter avtalen, kunne tolkes på ulike måter, og Høyesterett mente at det var egnet til å gi A inntrykk av at «det sentrale var at andre ikke kunne finne frem til tallene». [94] Hvilken plikt A hadde, var derfor uklar.

Det må her fremheves at Høyesterett, til tross uklarheten, ikke la avgjørende vekt på avtaletekstene. Det konkluderes med at nedtegningen «klart» ikke medførte grov uaktsomhet.[95] Dette tilsier at brudd på pliktene i seg selv ikke kan anses som grovt uaktsomt. Dette kan også si noe om selve normen for grov uaktsomhet; den er ikke direkte koblet til handlingsplikter i avtalen. Ved overtredelse skal det uansett foretas en helhetlig vurdering av handlemåten, og det må sees hen til alle forhold.

Dette har overføringsverdi også til tilfeller av BankID-misbruk. Også her er det vilkår for utstedelse og bruk. Brudd på pliktene her vil derfor ikke automatisk og i seg selv medføre grov uaktsomhet. Det må gjøres en helhetsvurdering. Dette harmonerer også med tolkningen av finansavtaleloven 2020 § 3-19 og hva som anses å være «rimelige forholdsregler» i HR-2020-2021-A. Dette harmonerer også godt med uttalelsen i PSD 2 om at det kreves «vesentlig grad av skjødesløshet».[96]

Ettersom nedtegningen i seg selv ikke ble ansett som grovt uaktsomt, ble spørsmålet i saken avgjort ved en samlet vurdering av hvor godt koden var kamuflert og hvordan den ble oppbe-

---

94 Rt. 2004 s. 499 avsnitt 28 og 29.

95 Rt- 2004 s. 499 avsnitt 31.

96 Direktiv 2015/236/EF fortalens punkt 72.

vart.[97] Denne vurderingen kan en pekepinn på hva som kreves ved nedtegning av passord til BankID-brikke.

I syvendesansen hadde A skrevet ned kodene kamuflert. Det var i tillegg notert ned flere firesifrede koder knyttet til andre bruksområder som ikke knyttet seg til kortene. Tre koder var notert på ulike sider, og disse var kamuflert ved å først benytte initialene til sine barn, deres fødselsdato og deretter koden. Det aktuelle kortet hadde koden 1275. Dette ble kamuflert ved sønnen Finns initialer og bursdagsdato slik at det kamuflerte notatet var «F/M» øverst på siden, og tallene «30041275».[98]

Det sentrale for vurderingen var «i hvilken grad koden var notert på en slik måte at det var mulig for andre å nyttiggjøre seg notatet for misbruk av kortet».[99] Det ble også fremhevet i vurderingen av om A var avskåret fra å skrive ned koden etter kortavtalen, at det for mange kortinnehavere ville være «meget vanskelig å praktisere en ordning fra å notere ned tallkoden».[100]

Også for BankID-brikker vil det kunne være «meget vanskelig å praktisere en ordning hvor man var helt avskåret fra å notere ned koden»,[101] spesielt når rettighetshaveren har flere koder å huske. Dette harmonerer også med vurderingen av hva som kan avtales i vilkårene, sett opp mot hva som er «rimelige forholdsregler» etter § 3-19, hvordan disse er tolket i HR-2020-2021-A og om vilkåret er i tråd med formålet.

Høyesterett tar ikke en selvstendig gjennomgang av kamufleringens eventuelle svakheter i seg selv, men viser til at en alminnelig person nok ville hatt vanskeligheter med å finne frem til de riktige sifrene blant det som var nedtegnet.[102] At spesielt interesserte, herunder kriminelle, har metoder for å knekke slike koder, er likevel noe den som har nedtegnet koden(e) må ta inn-

97 Rt. 2004 s. 499 avsnitt 31.
98 Rt. 2004 s. 499 avsnitt 35.
99 Rt. 2004 s. 499 avsnitt 33.
100 Rt. 2004 s. 499 avsnitt 30.
101 Rt. 2004 s. 499 avsnitt 30.
102 Rt. 2004 s. 499 avsnitt 36.

over seg når koden skal kamufleres. Når kamufleringen av kodene «med letthet [kunne] vært gjort vesentlig bedre», [103] kunne A bebreides. Isolert sett ble dette ansett uaktsomt.

Her skiller saken seg fra BankID-tilfellene. Koder til bankkort er ikke selvvalgte, i motsetning til BankID-koden. Det må sies å i seg selv være lettere å huske selvvalgte passord, noe som kan gjøre det mindre nødvendig å skrive ned for egen hukommelses skyld. Selv om det etter forarbeidene til den nye finansavtaleloven ikke i seg selv er uaktsomt å skrive ned passord tilknyttet brikken, skal det likevel gjøres på en slik måte at det ikke «enkelt» vil kunne misbrukes av tredjepart. Hvor «enkelt» det er å misbruke BankID-brikken, vil da måtte sees i sammenheng med oppbevaring av det nedskrevne passordet, herunder om det oppbevares i nærheten av brikken. Dette må også kunne sies å være en «rimelig forholdsregel» i mange tilfeller, da det ikke er spesielt byrdefullt. At det må gjøres en vurdering av om det var «mulig for andre å nyttiggjøre seg notatet», vil likevel ha overføringsverdi i vurderingen av nedtegning av passord tilknyttet BankID.

At det er «mulig for andre å nyttiggjøre seg notatet», betyr også at det er «enkelt» å gjøre det. Dette tilsier at det også må kunne stilles noen krav til kamuflering av passord til BankID-brikker når nedskrivingen oppbevares i nærheten av brikken. Dette vil være momenter som kan tale for grov uaktsomhet i disse tilfellene, hvor graden av kamuflering og oppbevaring i nærhet av brikken må vurderes.

Det må likevel bemerkes at det i Rt. 2004 s. 499 var tale om et bankkort, hvor alt som kreves for å gjennomføre misbruket er kode og kort, og at misbruket skjedde i utlandet. Dette kan tenkes å ha spilt inn i helhetsvurderingen. Ved misbruk av digital signatur kreves det både brikke, passord og personnummer. Det er ikke gitt at en tyv i utlandet verken vet hvordan BankID kan misbrukes eller kan skaffe seg tilgang til personnummer. Selv om det dommen pekes det på at profesjonelle tyver har erfaring med å knekke koder, og at dette må hensyntas ved nedtegning av koden, er det ikke gitt at det også for nedtegning av passord til BankID-brikker kreves like høye krav i utlandet.

[103] Rt. 2004 s. 499 avsnitt 36.

Om oppbevaringen skjer utenfor hjemmet, på et sted hvor rettighetshaveren har mindre kontroll, kan det tenkes at det raskere anses uaktsomt, eventuelt grovt uaktsomt, å ha en ukodet nedskriving sammen med brikken. Dette på samme måte som ved oppbevaring av selve brikken utenfor hjemmet, hvor det stilles strengere krav til oppbevaringen etter HR-2020-2021-A.

Det var nettopp oppbevaring utenfor hjemmet som var tilfellet i Rt. 2004 s. 499. Høyesterett peker på at også selve oppbevaringen av kode og kort er et sentralt moment. Kortet og syvendesansen ble oppbevart i en bebodd, låst leilighet som ikke var spesielt tyveriutsatt. Sett hen til oppbevaring av BankID-brikke på arbeidsplassen i HR-2020-2021-A stilles det her tilsvarende krav. Når det likevel kommer på spissen, pekes det mot tapsrisikoen, og at denne kunne vært fjernet på en «svært enkel måte». Holdt opp mot den dårlige kamufleringen var oppbevaringen derfor «ubetenksom».[104] I HR-2020-2021-A ble brikken alene oppbevart på et kontor, men da uten at det ble sannsynliggjort at passordet var nedskrevet i nærheten.

Etter en samlet vurdering anser Høyesterett det likevel utilstrekkelig til å overskride den høye terskelen, da det ikke er tale om at A har opptrådt «sterkt klanderverdig» eller at det var et «markert avvik fra det som fremstår som vanlig forsvarlig».[105] Dette fordi A kun var ute av leiligheten for en kort periode, og oppbevaringen hadde et midlertidig preg. At tapspotensialet var begrenset til kr. 10.000 spilte også inn.[106] Dette skiller seg klart fra BankID-tilfellene. Ved misbruk av BankID-brikke kan tapspotensialet bli nærmest uoversiktlig, og i alle tilfeller langt over de 10 000 kronene i saken. En for stor vektlegging av tapspotensialet ved fastsettelsen av uaktsomhetsterskelen vil raskt medføre så strenge sikringstiltak at det raskt vil hemme bruken til rettighetshaveren. Også her har tidsmomentet vekt, på samme måte som i HR-2020-2021-A.

Videre kan det utledes at kode og betalingsinstrument som et klart utgangspunkt ikke bør oppbevares samlet, selv om en slik oppbevaring er ubetenkelig for andre verdifulle gjenstander. En slik oppbevaring kan i seg selv øke tapsrisikoen, og dermed sannsynligheten for at tap oppstår. Risikoen kan enkelt elimineres ved å fjerne enten den nedskrevne koden eller betalingsinstrumentet. Dette taler for at terskelen raskt er nådd når disse oppbevares samlet, og at

---

104 Rt. 2004 s. 499 avsnitt 39.

105 Rt. 2004 s. 499 avsnitt 40.

106 Rt. 2004 s. 499 avsnitt 41.

det skal mindre til for å overstige terskelen dersom kamufleringen i tillegg er lett gjennomskuelig. Det må ut fra dette kunne utledes en regel om at kodebrikke og passord som den klare hovedregel ikke bør oppbevares samlet, og at der dette er tilfelle, vil konklusjonen fort kunne bli grov uaktsomhet. Spesielt om det gjøres over lengre tid. Dette harmonerer med uttalelsene i fortalen til PSD 2.

Dette utgangspunktet kan likevel nyanseres. Oppbevaringen hadde et klart midlertidig preg. Dette underbygges av at vurderingen «lett [kunne] ha blitt en annen» dersom A normalt gjorde dette i sitt eget hjem.[107] En havner da raskt i en situasjon hvor kunden både kunne og burde handlet annerledes.

Av dette kan det også utledes en vurdering av handlingsalternativer, som Høyesterett peker på når det uttales at tapsrisikoen på en «svært enkel måte kunne vært fjernet».[108] I As tilfelle ble det akseptert fordi oppbevaringen hadde et midlertidig preg. Det må likevel kunne tolkes som at terskelen senkes dersom kunden har enkle handlingsalternativer, men likevel har unnlatt å gjennomføre dem. Det må her også vektlegges at kortet og koden lå helt samlet. For BankID-brikker må det kunne legges til grunn en tilsvarende regel. Om det er gode grunner som taler for at en slik oppbevaring bør kunne aksepteres i det enkelte tilfellet må vurderes konkret, men som den klare hovedregel unngås, også i eget hjem.

Det hele beror imidlertid på en helhetsvurdering, hvor de ulike momentene må vurderes opp mot hverandre. I saken kunne A bebreides for dårlig kamuflering, noe som isolert sett var uaktsomt. Det er uklart om det samme ville vært tilfelle om koden var umulig å knekke. Det kan også tenkes at vurderingen ville vært en annen om A hadde foretatt ytterligere nedlåsning av kort og kode, selv om oppbevaringen var i en låst koffert i en forsvarlig lås, bebodd leilighet i Barcelona, som ikke var spesielt innbruddsutsatt. Dette vil også ha overføringsverdi til tilfeller av BankID-svindel. Om en er noe mer uforsiktig på ett av tiltakene, kan dette tilsi skjerpet forsiktighet og på andre tiltak. Eksempelvis dersom koden er skrevet ned uten å forsøke å kode den, kreves det større avstand mellom stedet passord er nedtegnet og kodebrikken.

---

[107] Rt. 2004 s. 499 avsnitt 40.

[108] Rt. 2004 s. 499 avsnitt 39.

Det siste som kan utledes er en generell uttalelse om at håndtering av betalingskort og kode må gis en «streng aktsomhetsvurdering ut fra likheten med håndtering av kontante penger».[109] Hvorfor det i disse tilfellene skal stilles strenge krav uttales ikke, men må sies å gi uttrykk for en skjerpet aktsomhetsterskel for oppbevaring av nedtegnet kode og kort. Dette skiller seg fra tilfeller av misbruk av BankID-brikker, som ikke på samme måte har en klar likhet med håndtering av kontante penger. Det kreves i tillegg tilgang på personnummer. At det pekes på at det potensielle tapet var begrenset til kr. 10.000, kan det synes som at tapsrisikoen gir grunnlag for skjerpet vurdering, og at vurderingen kunne blitt en annen om tapspotensialet var høyere. Dette korresponderer dårlig med terskelen for uaktsomhet i HR-2020-2021-A. I sistnevnte dom vektlegges det at en rettighetshaver kan forventes å være klar over risiko for misbruk og tap knyttet til urettmessige betalingstransaksjoner. Det kan likevel for en alminnelig rettighetshaver ikke anses nærliggende at BankID skal benyttes som eneste grunnlag for inngåelse av betydelige økonomiske avtaler. En kan derfor legge til grunn at det samme strenge utgangspunktet ikke nødvendigvis er fulgt opp i HR-2020-2021-A.

6 Når har rettighetshaveren handlet forsettlig?

6.1 Innledende bemerkninger

Etter finansavtaleloven 2020 § 3-20 fjerde ledd vil rettighetshaveren svare med en egenandel tilsvarende tapet tjenesteyteren kan gjøre gjeldende «i samsvar med ellers gjeldende rettsregler» dersom rettighetshaveren har misligholdt en eller flere av sine plikter etter § 3-19 første og annet ledd «forsettlig slik at rettighetshaveren måtte forstå at misligholdet kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».

Bestemmelsen er praktisk viktig. I tilfeller hvor det foreligger simpel eller grov uaktsomhet vil ansvaret være begrenset av egenandeler. Summene kan raskt bli svært mye høyere om rettighetshaveren har brutt sine plikter med forsett.

Tjenesteyteren kan etter dette gjøre gjeldende krav «i samsvar med ellers gjeldende rettsregler». Dette er det samme som er vurdert over i kapittel 3.3. Dette innebærer imidlertid at det ikke er hele tapet tjenesteyteren kan fremme mot rettighetshaveren. Egenandelen, og dermed

[109] Rt. 2004 s. 499 avsnitt 41.

rettighetshaverens ansvar, etter alminnelige erstatningsrettslige regler «kan lempes eller settes ned som følge av alminnelige regler om lemping eller skadelidtes medvirkning».[110] Denne summen, ferdig lempet, utgjør maksgrensen for rettighetshaverens egenandelsansvar.

Etter ordlyden er pliktbruddet «forsettlig» når rettighetshaveren «måtte forstå at misligholdet kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».

Ordlyden av «forsettlig» tilsier at en med viten og vilje har brutt sin plikt.

I det opprinnelige lovforslaget gjorde departementet en gjennomgang av hva som ligger i forsettskravet på privatrettens område. Et ubegrenset ansvar skulle være forbeholdt de tilfeller hvor «rettighetshaveren med forsett har satt seg utover tjenesteyterens sentrale interesser eller tilsidesetter sikkerhetsordninger som er avgjørende at blir fulgt ved normal bruk av signaturløsningen, for eksempel av sikkerhetsordningene (…) med forsett deles med andre».[111]

Departementet så likevel «ikke behov for å gå så langt som å kreve at forsettet må omfatte tapet».[112] En slik forståelse av forsettsbegrepet tilsier at rettighetshaverens forsett ikke knyttes til skadefølgen, men en mer snever forståelse av begrepet hvor en eller flere av pliktene brytes «med viten og vilje». Det ble da vist til den danske loven om betalinger § 100 femte ledd hvor det er hjemlet at forsett kun er aktuelt der betaleren har delt sin informasjon «under omstædigheder, hvor betaleren indså eller burde have indset» at det var risiko for misbruk. Dette er altså en løsning på tvers av departementets foreslåtte, hvor rettighetshaveren i det minste «utviste uaktsomhet når det gjelder følgene (misbruket) av pliktbruddet».[113]

Å innføre et krav om at skylden også måtte omfatte følgene ble ansett å stå i motstrid til PSD 2 artikkel 74 nr. 1, til tross for at dette er innført i EU-landet Danmark.[114] Typetilfellene hvor det potensielt kunne foreligge unnskyldelig rettsvillfarelse ville i så fall ha blitt vurdert etter

110 Innst. 104 L (2020-2021) s. 21.
111 Prop. 92 LS (2019-2020) s. 186.
112 Prop. 92 LS (2019-2020) s. 186.
113 Prop. 92. LS (2019-2020) s. 186.
114 Prop. 92 LS (2019-2020) s. 186.

alminnelige erstatningsrettslige regler, fremfor å fremgå som en begrensning i selve bestemmelsen.

I Stortinget ble dette endret. Mindretallets merknader, som oppnådde flertall i den endelige voteringen, forkastet departementets synspunkter. Det uttales at forsettskravet er oppfylt «bare dersom rettighetshaveren måtte forstå at mislighold av pliktene etter § 3-19 første og annet ledd kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».[115]

Stortingsflertallet legger videre til grunn at dette innebærer at «en rettighetshaver som fått bistand til å betale regninger på en slik måte at hjelperen får kjennskap til personlig sikkerhetsinformasjon, ikke nødvendigvis har handlet med forsett».[116] Det legges til domstolen(e) å avgjøre om rettighetshaveren ved sin handlemåte kan bebreides på en slik måte at pliktbruddet er forsettlig. Det er likevel ikke tilstrekkelig at uvedkommende har fått tilgang til personlig sikkerhetsinformasjon for å konstatere at vedkommende måtte forstå at det forelå nærliggende fare for misbruk.

Spesifikt trekkes det frem at personer som får bistand til å betale regninger, slik at hjelperen får kjennskap til den personlige sikkerhetsinformasjonen, «ikke nødvendigvis» har handlet forsettlig». I tillegg trekkes «eldre personer» og «personer som ikke kan språket godt» frem som grupper bestemmelsen særlig retter seg mot.[117] Situasjonene knytter seg til tilfeller hvor rettighetshaveren på en eller annen måte trenger bistand til eksempelvis å betale regninger, hvor hjelperen dermed får tilgang til den personlige sikkerhetsinformasjonen. Uttalelsene kan tolkes som at det er disse spesifikke tilfellene som nå ikke anses forsettlige når det ikke er en nærliggende fare for misbruk. En annen tolkning er at disse tilfellene er omfattet, men at det også kan tenkes øvrige tilfeller. Det illustrerer som et minimum at det skal gis et særlig vern for personer som trenger bistand for å bruke sin BankID. Det skal derfor mer til for å konstatere at handlingen er forsettlig, slik at vedkommende må bære hele tapet. I slike tilfeller vil

115 Innst. 104 L (2020-2021) s. 21.
116 Innst. 104 L (2020-2021) s. 21.
117 Innst. 104 L (2020-2021) s. 22.

rettighetshaveren heller kunne påberope ansvarsbegrensningen i tredje ledd,[118] altså grov uaktsomhet.

Dette gjør det nødvendig å vurdere nærmere hva som ligger i forsettsbegrepet sett i lys av ordlyden i bestemmelsen. Hvordan forsettsbegrepet er tolket i kontraktsretten kan kaste lys over hvordan det skal forstås også i finansavtaleloven.

6.2 Forsettlig pliktbrudd i kontraktsretten

Spørsmålet om hva som ligger i forsett i kontraktsretten er ikke helt klart, fordi forsett som skyldform først og fremst er utviklet innenfor strafferetten, men overført til kontraktsretten.[119] I strafferetten er forsett hjemlet i lov 20. mai 2005 om straff § 22, hvor det skilles mellom hensiktsforsett etter bestemmelsens bokstav a, sannsynlighetsforsett etter bokstav b og det såkalte dolus eventualis etter bokstav c. Gjerningspersonen skal vurderes ut fra sin oppfatning på gjerningstidspunktet etter strl. § 25 første ledd. Videre må forsettet i strafferetten knytte seg til handlingens følger eller de faktiske forholdene i det konkrete straffebud.

Forsettsbegrepet lar seg ikke direkte overføre til kontraktsretten fordi verken «delikts- eller kontraktserstatningsretten har strafferettens presise gjerningsbeskrivelser» og fordi ansvaret må bedømmes «etter en helhetsvurdering av kontraktsforholdet og de faktiske omstendigheter».[120] Det knytter seg derfor ulike måter å vurdere handlingsnormene for kontraktsretten og strafferetten, hvor handlingsnormene i kontraktsretten er situasjonsbestemte, mens for strafferetten er de lovbestemte.[121] Videre vil det i et kontraktsforhold være tale om forpliktelser som partene frivillig har inngått.

Nøyaktig hva som anses som et forsettlig kontraktsbrudd i kontraktsretten er omtvistet i juridisk teori.[122] For Lund og Augdahl er det avgjørende om selve misligholdet er forsettlig eller grovt uaktsomt. For Brunsvig og Kaasen er det avgjørende at forsettet også må knytte seg til medkontrahentens tap.

---

118 Innst. 104 L (2021-2022) s. 22.

119 Hagstrøm (2011) s. 479.

120 Hagstrøm (1996) s. 491.

121 Hagstrøm (2011) s. 479.

122 Augdahl (1978) s. 293, Lund (1964) s. 68, Brunsvig (1973) s. 354 og Kaasen (2005) s. 253.

Kaasen oppstiller det som en vurdering av klanderverdighet, hvor en beveger seg fra det uaktsomme, til det grovt uaktsomme og videre til det forsettlige pliktbruddet. Vurderingen må, argumenteres det for, knytte seg til om «leverandøren på kvalifisert klanderverdig måte setter sine interesser over medkontrahentens». Det avgjørende er om handlingen er «hensynsløs, sterkt illojal eller lignende».[123] Etter en slik vurdering må det gjøres en helhetlig vurdering av om selve handlingen i seg selv er klanderverdig, og om kontraktsparten har opptrådt illojalt og satt egne interesser over medkontrahentens.

For tilfeller ved misbruk av BankID, vil det være avgjørende hvordan en tolker forsettsbegrepet. Om en legger Augdahl og Lunds forståelse til grunn, vil selve pliktbruddet i seg selv medføre ansvar for hele beløpet dersom selve handlingen bak pliktbruddet er bevisst. Forsettet dekker da at det foretas et normbrudd. Ingen av forfatterne drøfter hvordan dette stiller seg om kontraktsparten er i rettsvillfarelse. Om Kaasen og Brunsvigs forståelse legges til grunn må forsettet også omfatte tapet for banken.

Kaasens vurdering knytter seg til fabrikasjonskontrakter, og omfatter avtaler som ofte er i milliardklassen. De avtales også mellom profesjonelle parter som har tilgang på god juridisk bistand i utformingen av kontrakten. Kaasen argumenterer videre med at det ved formuesskader er kjernen «klanderverdigheten, ikke leverandørens bevissthetsforhold alene» som må vurderes.[124] Selv om det er ulike rettsområder vil det harmonere dårlig med finansavtalen som forbrukerlov å legge den strengere forståelsen til grunn, altså at det er pliktbruddet isolert sett som er avgjørende. I så tilfelle kan en si at det kreves mindre av en alminnelig forbruker å havne i ansvar på grunn av forsettlig pliktbrudd enn en leverandør i en milliardavtale. Dette, sett sammen med uttalelsene i forarbeidene, taler derfor for en slik forståelse av forsettsbegrepet etter finansavtaleloven 2020.

6.3 «Måtte forstå» at det foreligger «nærliggende fare» for misbruk

Pliktbruddet er etter finansavtaleloven 2020 § 3-20 fjerde ledd kun forsettlig når rettighetshaveren «måtte forstå at misligholdet kunne innebære en nærliggende fare for at de elektroniske signaturfremstillingsdataene kunne bli misbrukt».

---

123 Kaasen (2005) s. 253.

124 Kaasen (2005) s. 253.

Ordlyden av «måtte forstå» tilsier at det må være bevissthet rundt at misbruket kan skje. Ordlyden av «nærliggende fare» tilsier videre at det må holdes som sannsynlig at pliktbruddet medfører misbruk. Det er imidlertid tilstrekkelig at misligholdet «kunne» innebære risiko for misbruk. Det tilsier at rettighetshaveren kun må ha kjennskap til at risikoen eksisterer. At faren må være «nærliggende» tilsier også at det ikke er tale om en hypotetisk mulighet for misbruk en gang i fremtiden. Det må være knyttet til den konkrete situasjonen, eller kort tid etter.

Forarbeidene gir liten veiledning i hvordan «måtte forstå» skal tolkes, utover at det vil samsvare med alminnelige regler om skadeserstatning hvor «forsett foreligger når skadevolderen holder det for mest sannsynlig («måtte forstå») at den aktuelle skaden vil inntreffe som et resultat av skadelidtes handling».[125] Her pekes det mot at skadevolderen, altså rettighetshaveren, må ha ansett det for mest sannsynlig at skaden ville inntreffe. Dette må sies å være noe utvidende sammenholdt med ordlyden av «måtte forstå», som ikke kan sies å tilsi at det holdes mer sannsynlig enn ikke at misbruk finner sted.

Hva som ligger i «måtte forstå» er drøftet i litteraturen. Hagstrøm peker på at et krav om sannsynlighetsforsett vil være «upraktikabelt» ettersom «parten lett måtte frifinnes for påstand om ikke å ha holdt følgene som sikre eller overveiende sannsynlig».[126] Som følge av dette utgangspunktet er det en rekke plasser i lovgivningen inntatt et krav under passusen «var eller måtte være kjent med» eller lignende, se eksempelvis lov 3. juli 1992 nr. 93 om avhending av fast eigedom § 3-7, lov 16. juni 1989 nr. 63 om håndverkertjenester m.m for forbrukere § 19 og lov 13. mai 1988 nr. 27 om kjøp §§ 17 andre ledd bokstav b og 19 første ledd bokstav b.

Etter kjøpsloven § 17 første ledd bokstav b heter det at tingen skal passe til et bestemt formål som selgeren «var eller måtte være kjent med» da kjøpet ble inngått. I forarbeidene uttales det at «Uttrykket «måtte være kjent med» innebærer at det ikke må foreligge noen rimelig unnskyldning for selgerens uvitenhet om det spesielle formålet, sml den liknende formulering «måtte skjøna» i gjeldsbrevloven § 18».[127] Av dette kan det utledes at det ikke er nødvendig å holde det overveiende sannsynlig, men at det i det konkrete tilfellet ikke må foreligge gode grunner til at den som har brutt plikten ikke vet at et foreligger opplysningssvikt.

---

125 Innst. 104 L (2021-2022) s. 22.

126 Hagstrøm (2011) s. 479.

127 Ot.prp. nr. 80 (1986-1987) s. 59.

Overført til våre aktuelle tilfeller vil det være vanskelig å trekke noen klar konklusjon for hva som gjelder. Ordlyden tilsier på den ene siden at rettighetshaveren må anse det som en mulighet at misbruk kan finne sted i det konkrete tilfellet. Å bevege seg inn i bevissthetsforestillinger som rettighetshaveren måtte ha på tidspunktet for pliktbruddet vil være vanskelig. Det vil derfor være nødvendig å gjøre en vurdering mer lik den som gjøres etter kjøpsloven § 17 første ledd bokstav b, og definert i forarbeidene der. Det må likevel sies å skulle noe mer til enn at det ikke foreligger noen «rimelig unnskyldning». Her kan også eksemplene i forarbeidene stå som eksempler. Ikke alle vil anse det som en nærliggende fare å oppgi personlig sikkerhetsinformasjon til sine nærmeste. Dette vil også kunne være tilfellet når en blir oppringt av noen som utgir seg for å være politiet eller banken. Det hele må da bero på en helhetsvurdering av hvordan det hele fremstår og hvor klanderverdig pliktbruddet er.

6.4 Rettsvillfarelse

Etter forarbeidene legges det til grunn at «personer som blir lurt til å oppgi personlig sikkerhetsinformasjon knyttet til de elektroniske signaturfremstillingsdataene, ikke vil få ansvaret for hele tapet som svindelen forårsaket».[128] Dette gjelder «eldre personer og personer som ikke kan språket godt, og som har behov for hjelp av andre til å betale regninger».[129] I disse tilfellene kan rettighetshaveren påberope seg egenandelen på 12 000 kroner.

Det kan tenkes tilfeller hvor rettighetshaveren ikke er klar over sine plikter etter avtalen. I slike tilfeller foreligger det rettsvillfarelse. Det er også en rimelig antakelse at ikke alle leser BankID-avtalen jevnlig. Ved rettsvillfarelse er det i utgangspunktet et objektivt ansvar for misligholdet.[130] Hagstrøm uttaler at «En effektiv beskyttelse av kontrakter og almene rettsregler tilsier imidlertid at hver kontraktspart har risikoen for sin egen rettsoppfatning (error juris semper nocet)».[131] En slik villfarelse kan likevel være unnskyldelig.

I noen situasjoner kan rettighetshaveren i god tro ha gitt fra seg passord og/eller annen sikkerhetsinformasjon til noen som utgir seg for å være en tillitsperson, for eksempel politiet eller

[128] Innst. 104 L (2020-2021) s. 22.
[129] Innst. 104 L (2020-2021) s. 22.
[130] Hagstrøm (2011) s. 527.
[131] Hagstrøm (2011) s. 527.

banken selv. Spørsmålet er om dette kan anses som unnskyldelig rettsvillfarelse i tråd med det som uttales i forarbeidene.

Spørsmålet ble vurdert i Finansklagenemnda i sak 2020/703. Her peker nemndas flertall først på at hele situasjonen bør tas i betraktning. Det legges til grunn at det er en forventning om at en alminnelig BankID-innehaver er innforstått med at engangskoder og passord ikke skal deles med uvedkommende. Det kan likevel ikke legges til grunn at dette uten videre også gjelder egen bank. Det ble da foretatt en helhetsvurdering av situasjonen.

Ettersom det ikke foreligger rettspraksis i lignende saker tydde nemnda til en systembetraktning av andre områder hvor rettsvillfarelse er aktuelt. Det blir pekt på at rettsvillfarelse kan utelukke skyld og ansvar etter straffeloven 2005 § 26. Videre at aktsom rettsvillfarelse også kan være aktuelt på privatrettensområde. Med henvisning til Rt. 1995 s. 1350, som gjaldt en tvist mellom eiendomsmegler og takstmann som følge av at en leilighet ikke kunne leies ut lovlig tok ikke Høyesterett stilling til rettsvillfarelse konkret fordi begge partene «kan bebreides for en eventuell rettsvillfarelse på dette punkt». Skyld ble i det konkrete tilfellet utelukket som følge av den eventuelle rettsvillfarelsen. Nemnda uttaler at det samme må gjelde «minst like sterkt i forbrukerforhold».

Selv om praksis fra Finansklagenemnda ikke har selvstendig rettskildemessig vekt kan avgjørelsen gi en pekepinn på hva som er relevante vurderingstema.

For det første kan det utledes at i tilfeller hvor det i utgangspunktet foreligger et forsettlig pliktbrudd, så kan dette bortfalle dersom rettighetshaveren er i rettsvillfarelse om sine plikter. Det kan også utledes at det må tas en helhetsvurdering av situasjonen. Dette vil være i tråd med Kaasens vurdering av klanderverdighet. Forsett vil da kunne være uaktuelt dersom handlingen ikke anses tilstrekkelig klanderverdig, situasjonen sett under ett.

Sett under ett må uttalelsene i forarbeidene kunne sies å omfatte tilfeller av rettsvillfarelse. Det må da tas en konkret helhetsvurdering av situasjonen, og en må vurdere graden av klanderverdighet.

Av uttalelsene i forarbeidene må det sies å kunne vektlegges subjektive forhold på skadevolders side. Personer som er i en sårbar situasjon vil kunne ha gode grunner til å gjøre som de

gjør. At passordet gis bort er ikke ensbetydende med at vedkommende verken vet at plikten brytes, eller at det er spesielt klanderverdig å gjøre det i det aktuelle tilfellet. I slike tilfeller vil rettighetshaveren ofte ikke ha forsett for skadefølgen, selv om vurderingen i seg selv er grovt uaktsom. Vedkommende kan da neppe sies å «bevisst og betydelig» ha satt seg utover motpartens sentrale interesser.[132]

Etter HR-2020-2021-A har det også relevans hvilke tiltak skadelidte har iverksatt. Det er fortsatt uavklart hvordan det vil slå ut på forsettsvurderingen dersom det samme er tilfelle.

7 Avsluttende refleksjoner

Misbruk av digital signatur har over flere år ført til at svindelofre har blitt holdt ansvarlig for lån tatt opp i deres navn. Selv om en på arket har et regresskrav mot svindler vil det ofte være svært vanskelig å inndrive dette. Enten fordi svindler er ukjent, eller fordi vedkommende ikke har økonomiske midler til å betale sine forpliktelser. I de tilfeller hvor svindler dømmes for forholdet fører det paradoksalt nok til at denne ikke tjener penger som kan gå med til å dekke kravet.

Som vist har utviklingen av forbrukervernet skjedd gradvis, og reguleringen av misbruk av digital signatur var derfor en naturlig forlengelse av dette vernet. Den digitale utviklingen har vært både ønsket og stimulert av både finansnæringen og offentlige myndigheter. Om forbrukere sitter med hele risikoen kan denne utviklingen bremses.

Ansvarsfordelingen er derfor viktig for å opprettholde tilliten til løsningene som tilbys – og som ikke kan sies å være helt valgfrie om en ønsker å ta del i løsningene som tilbys. Ved å flytte tapet over på finansinstitusjonene, som er nærmest til å iverksette tiltak for å forhindre svindel og kan pulverisere tapet, bidrar det til å opprettholde tilliten til den ønskede digitaliseringen.

Med avgjørelsen i HR-2020-2021-A kom det en viss avklaring, og imøtegåelse av den svært strenge aktsomhetsnormen som hadde utviklet seg over tid. Med avgjørelsen er det avklart at bankene ikke uten videre kan holde en rettighetshaver ansvarlig dersom det er enkle tiltak de

[132] Hagstrøm (2011) s. 481.

kan iverksette for å avverge svindelen. Også hvilke tiltak som kreves av en rettighetshaver synes moderert. Det er nå kommet en rettslig avklaring i hva som ligger i «alle rimelige forholdsregler» og hvor langt dette kan strekke seg.

Når hva som er uaktsomt er moderert, vil dette også få innvirkning i hva som anses grovt uaktsomt. Som vist i kapittel 5 er det klare holdepunkter for at det stilles strenge krav til oppbevaring av brikke og nedskrevet passord samlet.

Det som fremstår mest uavklart er likevel hvilke tilfeller som nå vil anses forsettlige. Selv om det er pekt på forhold som skal vektlegges, og at spesielt eldre personer og andre med språklige barrierer har fått et bedre vern, vil denne bestemmelsen i praksis være den viktigste. Hvilke pliktbrudd som anses forsettlige vil ha klart størst økonomisk betydning for den enkelte som utsettes for svindel. Her vil rettspraksis kunne peke ut kursen, nå med klare holdepunkter i forarbeidene og en ny ordlyd som vil kunne påvirke utfallet. Som jeg har argumentert for bør bestemmelsen tolkes i tråd med lovens formål.

Det som synes klart er at svindelmetoder stadig utvikles og rammer de svakeste. Som vist har utviklingen skjedd gradvis, hvor lovgiver kontinuerlig har hengt noe etter den digitale utviklingen. Nøyaktig hvilke svindelmetoder som utvikles kan enda ikke vites. Med større ansvar er det likevel grunn til å anta at finansinstitusjonene, av økonomiske hensyn, vil iverksette sterkere tiltak for å unngå svindel. Utviklingen vil likevel ikke stoppe. Spørsmålet er hvor raskt lovgiver reagerer med lovgivning når problemet eventuelt oppstår.

8 Litteraturliste

Lov- og forarbeidsregister:

1988 Lov 13. mai 1988 nr. 27 om kjøp (kjøpsloven)

1989 Lov 16. juni 1989 nr. 63 om håndverkertjenester m.m for forbrukere (håndverkertjenesteloven)

1992 Lov 3. juli 1992 nr. 93 om avhending av fast eigedom (avhendingslova)

1995 Lov 16. april 1995 nr. 53 om politiet (politiloven)

1999 Lov 17. juli 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven)

2005 Lov 20. mai 2005 nr. 28 om straff (straffeloven)

2018 Lov 1. juni 2018 nr. 23 om hvitvasking og terrorfinansiering (hvitvaskingsloven)

2020 Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven) (Ikke i kraft)

Ot. prp. nr. 80 (1986-1987) Om A Kjøpslov B Lov om samtykke til ratifikasjon av FN-konvensjonen om kontrakter for internasjonale løsørekjøp, vedtatt 11 april 1980

NOU 1994:19 Finansavtaler og finansoppdrag

Ot. prp. nr. 41 (1998-1999) Om lov om finansavtaler og finansoppdrag (finansavtaleloven)

NOU 2008:21	Nettbankbasert betalingsoverføring. Utredning nr. 21 fra Banklovkommisjonen
Ot. prp. nr. 94 (2008-2009)	Om lov om endringer i finansavtaleloven mv. (gjennomføring av de privatrettslige bestemmelsene i direktiv 2007/64/EF
Meld.St.27 (2015-2016)	Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet
Prop. 92 LS (2019-2020)	Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014
Innst. 104 L (2020-2021)	Innstilling til Stortinget fra justiskomiteen Prop. 92 LS (2019-2020)

EU-direktiv:

93/13/EØF	Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler
2007/64/EF	Europapalaments- og rådsdirektiv 2007/64/EF av 13. november 2007 om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, og 2006/48/EF samt oppheving av direktiv 97/5/EF [Betalingstjenestedirektivet, PSD 1]
2015/2366	Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betailngstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og

forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF [Betalingstjenestedirektivet, PSD 2]

Rettspraksis:

Rt. 1989 s. 1318
Rt. 1995 s. 1350
Rt. 1997 s. 1807
Rt. 2004 s. 499
HR-2020-2021-A
LB-2016-43622
LB-2014-13514
TGJOV-2017-170313
TOSLO-2018-180834
TGLOM-2020-156504

Fra Finansklagenemnda:

FinKN-2014-550
FinKN-2020-73

Avtaler:

BankID «Avtalevilkår for PersonBankID og AnsattBankID – PDS» 21.5.19 https://www.bankid.no/globalassets/dokumenter/apne-sider/bankid/dnb_pds_personal-v1.1.pdf hentet 17.5.21

Litteratur og juridisk teori:

Augdahl (1978) Augdahl, Per. *Den norske obligasjonsretts almindelige del*. 5. utg., Oslo: Tano Aschehoug, 1978.

Brunsvig (1973) Brunsvig, Per. *Konstruksjonsansvar ved bygging av skip*. Oslo: Universitetsforlaget, 1973.

Eckhoff (2001) — Eckhoff, Torstein. *Rettskildelære.* 5. utg., ved Jan E. Helgesen, Oslo: Universitetsforlaget 2001.

Fredriksen og Mathisen (2019) — Haukeland Fredriksen, Halvard og Mathisen, Gjermund. «EU-rett som norsk rettskilde». I *Juridisk metode og tenkemåte.* Alf Petter Høgberg og Jørn Øyrehagen Sunde red., Oslo: Universitetsforlaget, 2019 s. 386-419.

Giertsen (2014) — Giertsen, Johan. *Avtaler.* 3. utg., Oslo: Universitetsforlaget, 2014.

Hagstrøm (2011) — Hagstrøm, Viggo. *Obligasjonsrett.* 2. utg., Oslo: Universitetsforlaget, 2011.

Hagstrøm (1996) — Hagstrøm, Viggo. «Om grensene for ansvarsfraskrivelse, særlig i næringsforhold». *Tidsskrift for rettsvitenskap* nr. 4 1996. s. 421-518.

Hov (2002) — Hov, Jo. *Avtaleslutning og ugyldighet. Kontraktsrett I.* 3. utg., Oslo: Papinian 2002.

Justis- og beredskapsdepartementet — *Høringsnotat – revisjon av finansavtaleloven.* September 2017.

Kaasen (2005) — Kaasen, Knut. «Ansvarsbegrensning i fabrikasjonskontrakter». I *Industribygging og rettsutvikling – juridisk festskrift i anledning Hydros 100-årsjubileum*. Biller, Odd Ivar, Brannsten, Erik, Brautaset, Are og Hasaas, Olav red., Oslo: Fagbokforlaget, 2005. s. 233-258.

Kjelland (2016) — Kjelland, Morten. *Erstatningsrett – en lærebok.* 1. utg., Oslo: Universitetsforlaget, 2016.

Kjørven (2020) Kjørven, Marte. «BankID-svindel – HR-2020-2021-A». *Nytt i privatretten* nr. 4 2020.

Lilleholt (2017) Lilleholt, Kåre. *Kontraktsrett og obligasjonsrett*. 1. utg., Oslo: Cappelen Damm Akademisk, 2017.

Lund (1964) Lund, Ole. «Standardkontrakter, bilsalg og preseptoriske regler». *Lov og rett* Årg. 91, nr. 2 1964, s. 66-81.

Nygaard (2007) Nygaard, Nils. *Skade og ansvar*. 6. utg., Bergen: Universitetsforlaget, 2007.

Nettsider:

Advokatbladet «Mener ny finansavtalelov kunne reddet svindelofre fra erstatningsansvar etter ID-tyveri». https://www.advokatbladet.no/id-tyveri-norsis/mener-ny-finansavtalelov-kunne-reddet-svindelofre-fra-erstatningsansvar-etter-id-tyveri/147199 [Hentet 17.5.21]

E24 Professor mener ID-svindel kan være lønnsomt for bankene. https://e24.no/naeringsliv/i/LABV74/professor-mener-id-svindel-kan-vaere-loennsomt-for-bankene [Hentet 17.5.21]

BankID «Om oss» https://www.bankid.no/privat/om-oss/ [Hentet 28.4.2021]

jussbuss.no

Juss-Buss
Skippergata 23
0154 Oslo
tlf: 22 84 29 00
faks:22 84 29 01
www.jussbuss.no