UiO : Det juridiske fakultet

Ansvarsfordelingen mellom forbruker og bank ved ikke godkjente betalingstransaksjoner

Grensen for grovt uaktsomme og forsettlige pliktbrudd ved misbruk av elektroniske betalingsinstrumenter etter ny finansavtalelov

Kandidatnummer: 572

Leveringsfrist: 18. mai 2021

Antall ord: 17989

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Den økende digitaliseringen av samfunnet medfører at vi i stor grad har blitt avhengige av elektroniske betalingsløsninger. Betalingskort erstatter kontanter, og bare i 2019 ble det utgitt 13,7 millioner nye betalingskort i Norge.[1] Digitaliseringen bidrar til en gradvis utfasing av den fysiske banken og har på kort tid endret måten vi gjennomfører betalingstransaksjoner på. Enorme pengesummer er nå i omløp ved bruk av elektroniske betalingsløsninger som betalingskort og nettbank, noe som innebærer en betydelig risiko for økonomisk tap ved en tredjepersons misbruk av disse. Ved utgangen av 2020 ble det rapportert om tap knyttet til misbruk av betalingskort tilsvarende 147,5 millioner kroner og tap knyttet til nettbanksvindel tilsvarende 355 millioner kroner.[2] Ofte er det vanskelig å oppdrive svindleren og holde vedkommende ansvarlig, og spørsmålet blir da om det er kunden eller betalingstjenesteyteren som skal bære tapet.

Temaet for denne avhandlingen er reglene om tapsfordelingen mellom kunden og betalingstjenesteyteren ved ikke godkjente betalingstransaksjoner etter finansavtaleloven (2020) § 4-30.[3] Loven ble vedtatt av Stortinget 1. desember 2020,[4] og ble sanksjonert av Kongen i statsråd 18. desember samme år.[5] Ved lovens ikrafttredelse vil den avløse finansavtaleloven (1999),[6] men tidspunktet for ikrafttredelse er enda ikke satt, jf. § 8-1.[7]

Finansavtaleloven (2020) § 4-30 gjennomfører artikkel 74 i det reviderte betalingstjenestedirektivet, heretter PSD 2.[8] Utgangspunktet etter § 4-30 første ledd er at betalingstjenesteyteren er ansvarlig for tap som skyldes en ikke godkjent betalingstransaksjon. Dette objektive ansvaret modereres i de påfølgende ledd. Etter annet ledd svarer kunden for en egenandel på inntil 450 kroner hvis det økonomiske tapet skyldes tap, tyveri eller uberettiget tilegnelse av et «betalingsinstrument». Dette gjelder imidlertid ikke dersom kunden ikke kunne forhindret dette på forhånd og heller ikke har opptrådt svikaktig. Etter tredje ledd svarer kunden for hele det økonomiske tapet dersom kunden «grovt uaktsomt» har unnlatt å etterfølge de pliktene som følger av §§ 4-23 første ledd og 4-24 første ledd. Kunden svarer imidlertid kun for en egenandel på inntil 12 000 kroner dersom betalingstransaksjonen har skjedd ved bruk at et «elektronisk betalingsinstrument». Etter fjerde ledd svarer kunden for hele tapet dersom

[1] Norges Bank (2020) s. 10.

[2] Finanstilsynet (2021) punkt 4.2 og 4.3.

[3] Lov av 18. desember 2020 nr. 146 om finansavtaler.

[4] Lovvedtak 24 (2020-2021).

[5] Regjeringen (2020).

[6] Lov av 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag.

[7] Det antas at loven vil tre i kraft tidlig i 2022, jf. Meld. St. 31 (2020-2021) s. 45.

[8] Direktiv (EU) 2015/2366.

vedkommende «forsettlig» har misligholdt sine plikter på en slik måte at kunden «måtte forstå» at dette kunne innebære en «nærliggende fare» for misbruk.

Avhandlingen tar sikte på å besvare følgende spørsmål: Hva utgjør henholdsvis grovt uaktsomme og forsettlige pliktbrudd etter finansavtaleloven (2020) § 4-30? Som den nærmere vurderingen av disse spørsmålene i kapittel 3 og 4 vil vise, oppstår også spørsmålet om betalingstjenesteyteren i lys av forbrukervernhensyn bør bære en større del av tapet ved ikke godkjente betalingstransaksjoner. Dette vil behandles avslutningsvis i kapittel 5.

1.2 Rettskildebildet og metode

1.2.1 Metode

Avhandlingen tar for seg kommende rett på området for ikke godkjente betalingstransaksjoner, hvor innholdet i reglene etter finansavtaleloven (2020) vil klarlegges ved bruk av alminnelig juridisk metode. Det vil tas utgangspunkt i typetilfeller av ikke godkjente betalingstransaksjoner for å klarlegge skyldgrensene, slik som såkalt «phishing», «vishing» og tredjepersons misbruk av betalingskort og kode, se nærmere om typetilfellene i punkt 1.3.

Et særskilt spørsmål er i hvilken grad rettskilder i tilknytning finansavtaleloven (1999), herunder rettspraksis og nemndspraksis, vil være relevant for å klarlegge innholdet i reglene etter finansavtaleloven (2020). Dette vil behandles nærmere under punkt 1.2.3. Rettskildeverdien av Finansklagenemndas praksis vil behandles under punkt 1.2.4.

1.2.2 Sentrale rettskilder

Den sentrale rettskilden er finansavtaleloven (2020), som avløser gjeldende finansavtalelov (1999). Ettersom loven er ny og enda ikke trådt i kraft, vil den nærmere forståelsen av innholdet i første rekke måtte bygge lovens ordlyd og forarbeider.[9] Loven gjennomfører PSD 2 i norsk rett, og i tillegg til de nasjonale rettskildene vil direktivet være en sentral rettskilde. Mer generelt vil alminnelig kontraktsrett og erstatningsrett supplere rettskildebildet på området for avhandlingens tema.

Det folkerettslige presumsjonsprinsippet innebærer at norsk rett skal være i samsvar med EØS-retten, og medfører at EØS-rettslige kilder på generelt grunnlag er relevante og sentrale for tolkningen av norsk rett.[10] Finansavtaleloven (2020) må tolkes i samsvar med PSD 2, som med enkelte unntak er et fullharmoniseringsdirektiv.[11] Dette medfører at direktivets

[9] Skoghøy (2018) s. 78.

[10] Bergo (2019) s. 231.

[11] PSD 2 artikkel 107.

bestemmelser utgjør en absolutt norm for statenes internrettslige regulering.[12] EU- og EØS-rettslige kilder som er relevante for forståelsen av direktivet vil da også være relevante for forståelsen av finansavtaleloven (2020). Det følger imidlertid av fortalen til PSD 2 punkt 72 at «[b]eviset for og graden af den påståede forsømmelse bør generelt vurderes i henhold til national ret». Direktivet innrømmer dermed at den nærmere grensedragningen av skyldgradene som utgangspunkt bør baseres på nasjonale rettstradisjoner. Forsett nevnes ikke uttrykkelig, men i mangel på en anvisning på noe annet er det nærliggende at direktivet legger opp til en tilsvarende forståelse for forsettbegrepet.

Dette må imidlertid leses i lys av EU- og EØS-rettens overordnede mål om ensartethet.[13] I fortalen til PSD 2 punkt 6 følger det at direktivet skal «sikre ensartet anvendelse af de retlige rammer i hele Unionen», som uttrykker EU- og EØS-rettens homogenitetsmålsetting. Målet om en ensartet anvendelse av EU- og EØS-rettens regelverk medfører at medlemsstatene ikke kan eller bør stå helt fritt til å definere hvordan skylbegrepene i direktivet skal forstås i nasjonal rett. I mangel på autorative rettskilder fra EU og EØS i tilknytning skyldbegrepene, så vil likevel nasjonale rettskilder måtte tillegges avgjørende vekt.

EU- og EØS-rettslig tolkning styres av formålsbetraktninger, slik at formålet med bestemmelsene fremmes i størst mulig grad.[14] PSD 2 tar sikte på å sikre en rekke formål, herunder utviklingen av et integrert indre marked for trygge elektroniske betalingsløsninger og sikre et høyt nivå av forbrukerbeskyttelse ved bruken av disse betalingstjenestene.[15] Hensynet til forbrukeren og forbrukerbeskyttelse vil av den grunn være en sentralt ved fortolkningen av de relevante bestemmelsene i finansavtaleloven (2020).

Praksis fra andre EU-land vil brukes for å belyse hvordan disse landene har tolket og forstått de tilsvarende reglene i deres respektive nasjonale lovgivning. På grunn av plasshensyn og språklige begrensninger, vil det hovedsakelig brukes praksis fra Danmark, Sverige og Storbritannia, som alle har implementert PSD 2 i nasjonal rett.[16]

1.2.3 Forholdet mellom gammel og ny finansavtalelov

Her vil det i korthet redegjøres for de sentrale endringene i ny finansavtalelov. Også relevansen av tidligere praksis vil belyses, som hovedsakelig beror på en tolkning av ordlyden og hvorvidt

[12] Sejersted (2011) s. 299.

[13] EØS-avtalens fortale punkt 16.

[14] Fredriksen og Mathisen (2018) s. 308.

[15] Fortalen til PSD 2 punkt 5 og 7.

[16] Storbritannia er fra 1. januar 2021 ikke lenger medlem av EU, men avgjørelsene som her brukes er avsagt før dette tidspunkt.

denne utgjør et brudd med tidligere lovgivning. Dernest beror relevansen på en tolkning av forarbeidene og hvorvidt de gir uttrykk for at gjeldende rett endres.[17]

Finansavtaleloven (2020) § 4-30 bygger videre på reguleringen av ikke godkjente betalingstransaksjoner i finansavtaleloven (1999) § 35, som i sin tid gjennomførte PSD 1.[18] Kundens ansvar for forsettlige pliktbrudd følger av finansavtaleloven (2020) § 4-30 fjerde ledd, som i likhet med finansavtaleloven (1999) § 35 tredje ledd fastslår at ansvarsbegrensningene bortfaller. Det følger imidlertid av finansavtaleloven (2020) § 4-30 fjerde ledd at kunden i tillegg «måtte forstå at misligholdet kunne innebære en nærliggende fare for at betalingsinstrumentet kunne bli misbrukt». Dette innebærer en presisering av forsettkravet sammenlignet med tidligere regulering. Rettskilder etter finansavtaleloven (1999) er dermed ikke nødvendigvis relevante for forståelsen av forsettbegrepet etter finansavtaleloven (2020). Hva som nærmere ligger i forsettkravet, vil bli redegjort for i kapittel 4.

Ordlyden i § 4-30 tredje ledd om grovt uaktsomme pliktbrudd gjenspeiler ordlyden i finansavtaleloven (1999) § 35 tredje ledd, som tilsier at rettstilstanden på dette punkt videreføres. Forarbeidene slår fast at finansavtaleloven (2020) § 4-30 «erstatter med noen endringer» bestemmelsen i finansavtaleloven (1999) § 35.[19] Endringene knytter seg hovedsakelig til egenandelssatsene, uten at det nærmere kommenteres om grensen for grovt uaktsomme pliktbrudd skal praktiseres annerledes enn etter finansavtaleloven (1999). Av innstillingen følger det at «[d]e nevnte reglene om misbruk av konto og betalingsinstrument innebærer med noen endringer en videreføring av § 35 i gjeldende lov».[20] De vedtatte endringene er de samme som nevnt over etter proposisjonen, og heller ikke her kommenteres det om grensen for grovt uaktsomme pliktbrudd skal praktiseres annerledes. Tvert imot taler innstillingen om en «videreføring» av reglene i finansavtaleloven (1999) § 35.

Forarbeidene gir med andre ord ikke uttrykk for at den materielle vurderingen av hva som utgjør et grovt uaktsomt pliktbrudd skal praktiseres annerledes etter finansavtaleloven (2020). Av den grunn kan praksis og øvrige rettskilder etter finansavtaleloven (1999) være relevante rettskilder for å klargjøre hva som utgjør grov uaktsomhet etter finansavtaleloven (2020) § 4-30 tredje ledd.

[17] Mæhle og Aarli (2019) s. 129 flg.

[18] Direktiv 2007/64/EF, som erstattes av PSD 2.

[19] Prop. 92 LS (2019–2020) s. 172.

[20] Innst. 104 L (2020-2021) s. 7.

1.2.4 Finansklagenemndas praksis som rettskildefaktor

Finansklagenemnda er et bransjebasert tvisteløsningsorgan som løser tvister mellom finansinstitusjoner og deres kunder.[21] I denne avhandlingen siktes det til Finansklagenemnda Bank, som løser tvister innenfor sektorene bank, finans og verdipapirfond.[22] Avgjørelsene er rådgivende og uten rettslig bindende virkning.[23] Dette medfører at nemndas avgjørelser i tråd med alminnelig juridisk metode har liten vekt sammenlignet med avgjørelser fra de tradisjonelle domstolene.

Høyesterett har ikke tatt stilling til rettskildeverdien av Finansklagenemndas praksis. I Rt. 1984 s. 248 belyste Høyesterett imidlertid et beslektet spørsmål når det uttales at praksis fra Næringslivets Konkurranseutvalg ikke binder domstolene, men at «det ofte vil være naturlig å tillegge dem betydelig vekt». Konkurranseutvalget avgir rådgivende uttalelser, i likhet med Finansklagenemnda.[24] Hagstrøm fremhever med henvisning til denne dommen at det er grunn til å tro at det samme utgangspunktet vil bli lagt til grunn for Finansklagenemnda.[25] Tilsvarende synspunkter kan utledes av Rt. 1987 s. 744, hvor retten uttalte seg om rettskildeverdien til Forsikringsklagenemndas praksis, som i dag er en del av Finansklagenemnda. Høyesterett fremhever på side 748 at en etablert og langvarig partspraksis og nemndspraksis etter omstendighetene må tillegges betydelig vekt.

Det er imidlertid flere tiår siden disse avgjørelsene ble avsagt, og det er ingen garanti for at Høyesterett i dag vil innta samme standpunkt for Finansklagenemndas vedkommende. Eksempelvis kan Høyesteretts avgjørelse i HR-2020-2401-A trekkes frem, hvor domstolen i en sak om erstatning for forsinket flyreise kom til at det utenfor de lovregulerte tilfellene ikke gjelder noen generell regel om reklamasjonsplikt, uten å i det hele tatt nevne etablert praksis fra Transportklagenemnda som hadde lagt til grunn et motsatt resultat.[26]

På denne bakgrunn legges det til grunn at praksis fra Finansklagenemnda har begrenset rettskildeverdi, særlig i forhold til de tradisjonelle domstolene.[27] Hvorvidt nemdspraksis skal vektlegges, beror i hovedsak på avgjørelsenes argumentasjonsverdi, hvor etablert praksisen er og i hvilken grad den understøttes av øvrige rettskilder.[28]

---

[21] Vedtekter for Finansklagenemnda punkt. 1.1. og 1.3.

[22] Avtale om Finansklagenemnda punkt 1.

[23] Avtale om Finansklagenemnda punkt 3 bokstav k.

[24] Vedtekter for Næringslivets Konkurranseutvalg (2017) § 1.

[25] Hagstrøm (2011) s. 58.

[26] Se eksempelvis FLYKN-2017-3300, FLYKN-2018-2518 og FLYKN-2019-145.

[27] Hallsteinsen (2018) s. 334.

[28] Andenæs (2009) s. 98 og Hagstrøm (2011) s. 58.

1.3 Forbrukerrettet svindel - typetilfellene

Vurderingen av skyldgrensene i kapittel 3 og 4 vil ta utgangspunkt i utvalgte typetilfeller av misbruk av betalingsinstrumenter, slik som «phishing», «vishing» og tredjepersons misbruk av betalingsinstrument og tilhørende kode eller passord. Disse formene for svindel er blant de vanligste tilfellene av misbruk av betalingsinstrumenter i Norge.[29]

«Phishing» er en form for sosial manipulering hvor svindleren utnytter kundens fristelser, frykt, tillit eller opplevelsen av tidspress for å «fiske» etter informasjon om et betalingsinstrument og personlige sikkerhetsinformasjon.[30] Vanligvis skjer dette gjennom en e-post eller tekstmelding som er lik eller identisk som en reell melding.[31] «Vishing» er en særskilt form for «phishing» hvor svindlerne ringer kunden og forleder vedkommende til å oppgi informasjon om deres betalingsinstrumenter.[32] Det er også tilknyttet en betydelig risiko for svindel når kunden skriver ned passord og PIN-koder. Med mindre slik informasjon oppbevares totalt utilgjengelig for tredjepersoner vil det medføre en risiko for at den kommer på avveie, enten til nærstående eller andre uvedkommende.

Disse typetilfellene vil danne grunnlaget for den nærmere vurderingen av grensedragningen for hva som utgjør grov uaktsomhet og forsett etter finansavtaleloven (2020) § 4-30. Praksis fra Finansklagenemnda vil være sentralt ved den nærmere vurderingen av typetilfellene, ettersom slike saker ofte blir behandlet i nemnda. I den grad det finnes tilgjengelig praksis fra de alminnelige domstolene, vil dette inngå i vurderingen av typetilfellene i tillegg til den tilgjengelige nemdspraksisen.

1.4 Begrepsavklaringer og avgrensninger

Finansavtaleloven (2020) benytter uttrykkene «betalingstjenesteyter» og «kunde» ved omtalen av partene ved ikke godkjente betalingstransaksjoner, og disse vil brukes tilsvarende i denne avhandlingen. Ettersom loven etter § 1-9 er fravikelig utenfor forbrukerforhold, avgrenses avhandlingen til å omhandle forbrukertilfellene. Med «kunde» siktes det dermed til en forbruker.

Avhandlingen gjelder videre tredjepersons misbruk av betalingsinstrumenter, slik at kundens ansvar ved dens egen svikaktige opptreden etter § 4-30 annet ledd ikke vil behandles. Dette utelukker også en nærmere behandling av tap som skyldes betalingstjenesteyteren selv, jf.

[29] Finanstilsynet (2021) s. 32, 35 og 36.

[30] Næringslivets sikkerhetsråd (2020) s. 57.

[31] NorSIS (2020) s. 21.

[32] Næringslivets sikkerhetsråd (2020) s. 56.

§ 4-30 femte ledd. Kundens ansvar for den objektive egenandelen i § 4-30 annet ledd blir ikke nærmere behandlet, og av plasshensyn vil heller ikke bevisreglene i § 3-7 bli behandlet.

Avhandlingens tema innebærer også en avgrensning mot misbruk av BankID i form av elektronisk signatur, som etter ny finansavtalelov er regulert i § 3-20.[33] Til slutt presiseres det at denne avhandlingen gjelder misbruk av «elektroniske betalingsingsinstrumenter», ettersom slikt misbruk utgjør de vanligste formene for ikke godkjente betalingstransaksjoner. I det videre vil kun uttrykket «betalingsinstrumenter» benyttes.

[33] BankID kan også brukes til å gjennomføre betalingstransaksjoner, se punkt 2.3.2.

2 Generelt om reguleringen av ikke godkjente betalingstransaksjoner

2.1 Innledning

Ansvarsfordelingen avhenger av hvilken grad av skyld kunden har utvist ved pliktforsømmelsen. Utgangspunktet er § 4-30, men skyldvurderingen beror på et samspill av flere bestemmelser hvor den sentrale er kundens plikter etter § 4-23, se nærmere under punkt 2.3. Virkningen av at ansvarsbegrensningene påberopes er at betalingstjenesteyteren «straks, og senest innen utgangen av den påfølgende virkedagen» plikter å tilbakebetale beløpet og rentetapet fratrukket egenandelen i § 4-30, jf. § 4-32 første ledd. Tilbakebetalingsplikten gjelder imidlertid ikke ved mistanke om svik og det reises sak innen fire uker fra kundens skriftlige klage, jf. § 4-30 annet ledd.

Forarbeidene til finansavtaleloven (1999) redegjør nærmere for hensynene bak ansvarsbegrensningene. Samfunnsøkonomiske hensyn er den bærende begrunnelse for at kundens ansvar skal begrenses avhengig av utvist skyld.[34] Det er gunstig for samfunnet å legge til rette for bruk av elektroniske betalingsinstrumenter uten at kunden må påta seg en betydelig økonomisk risiko. Kunden har begrenset mulighet til å eliminere risikoen, samtidig som betalingstjenesteyteren kan pulverisere tapet. Ansvarsbegrensningene medfører videre at betalingstjenesteyteren oppfordres til å prioritere sikkerhet og betryggende betalingsløsninger.

Samtidig som et mål med PSD 2 er å fremme sikrere betalingsløsninger og styrke forbrukervernet, skal det også åpne for nyskapning og redusere kostnadene ved bruk av betalingstjenester.[35] Flere betalingstjenesteytere har fremhevet at en konsekvens av å lempe for mye av ansvaret over på finansinstitusjonene vil være at risikoen for misbruk øker og tilliten til elektroniske betalingsløsninger blir mindre.[36] At kunden pålegges et ansvar er dermed en forlengelse av erstatningsrettslige prevensjonshensyn, hvor kunden vil ha et økonomisk press til å redusere sin risikoskapende adferd.[37]

Ved avveiningen av disse hensynene har lovgiver konkludert at kunden skal ha en begrenset tapsrisiko ved ikke godkjente betalingstransaksjoner, med unntak for de forsettlige pliktbruddene. Dette reiser to sentrale spørsmål, nemlig hva som utgjør en ikke godkjent betalingstransaksjon og hva som er kundens plikter, som vil behandles videre i punktene 2.2 og 2.3.

[34] Ot.prp.nr. 94 (2008-2009).

[35] Prop. 92 LS (2019-2020) s. 19.

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

[37] Kjelland (2019) s. 32.

2.2 Hva er en ikke godkjent betalingstransaksjon?

Virkeområdet for finansavtaleloven (2020) § 4-30 er «ikke godkjente betalingstransaksjoner». Ansvarsbegrensningene er dermed betinget av at det for det første har skjedd en betalingstransaksjon og for det andre at denne betalingstransaksjonen ikke er godkjent. Dette gjør det nødvendig å avklare betydningen av disse begrepene.

Uttrykket «betalingstransaksjon» er legaldefinert i § 1-5 sjette ledd som «en handling som iverksettes av betaleren eller på dennes vegne eller av betalingsmottakeren for å innbetale, overføre eller ta ut betalingsmidler [...]».[38] Det må altså initieres en betaling, overføring eller et uttak, hvor gjenstanden for denne handlingen må være «betalingsmidler». Med «betalingsmidler» menes «pengesedler og mynter samt innskudd og kreditt på konto og elektroniske penger som definert i finansforetaksloven § 2-4 annet ledd», jf. § 1-5 fjerde ledd.

Dernest må denne betalingstransaksjonen ikke være «godkjent». Det følger av § 4-2 første ledd at en betalingstransaksjon er godkjent «bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres».[39] Definisjonen stiller ingen nærmere krav til innholdet i samtykket, utover at samtykket «skal gis i den formen og på den måten som er avtalt mellom betaleren og betalingstjenesteyteren», jf. § 4-2 annet ledd. Forarbeidene slår fast at bestemmelsen viderefører gjeldende rett og viser til avtalerettslige utgangspunkter når det uttales at et «samtykke kan være generelt utformet og gjelde et bredt spekter av tjenester, eller det kan være mer avgrenset og konkretisert. Det er mot denne bakgrunnen regler om samtykkekrav i finansavtaleloven må forstås».[40] Hva som utgjør et rettslig bindende samtykke etter § 4-2 må forstås på bakgrunn av avtalerettslige regler om hva som utgjør en rettslig bindende disposisjon. Dersom kunden skulle bestride at et samtykke er gyldig, må spørsmålet løses etter avtalelovens bestemmelser om ugyldige viljeserklæringer i kapittel 3 og ulovfestede regler om ugyldige viljeserklæringer.[41]

Et særlig spørsmål oppstår i de tilfellene der kunden blir lurt til å selv gjennomføre betalingstransaksjonen, eksempelvis ved såkalt «kjærlighetssvindel» eller fakturasvindel.[42] Her iverksetter kunden selv betalingstransaksjonen og angir hvem som skal være mottaker av pengene. Betalingstjenesteyteren er etter § 4-28 første ledd ansvarlig overfor betaleren for «korrekt gjennomføring» av en betalingstransaksjon som iverksettes av betaleren.[43] Betalingstransaksjonen er korrekt gjennomført når betalingsoppdraget gjelder en

[38] Tilsvarende PSD 2 artikkel 4 nr. 5.

[39] Tilsvarende PSD 2 artikkel 64.

[40] Prop. 92 LS (2019-2020) s. 276, jf. s. 279.

[41] Lov av 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer.

[42] Finanstilsynet (2020) s. 48.

[43] Tilsvarende PSD 2 artikkel 89.

betalingsmottaker som det angitte kontonummeret eller annen entydig identifikasjon utpeker, jf. § 4-26 første ledd.[44] Betalingstjenesteyteren trenger følgelig kun å sørge for at det er samsvar mellom det angitte kontonummeret og den *faktiske* betalingsmottakeren.[45] Når kunden selv angir slik betalingsinformasjon, plikter betalingstjenesteyteren å gjennomføre betalingstransaksjonen i tråd med den oppgitte betalingsinformasjonen. Kunden har da selv godkjent betalingstransaksjonen, til tross for å ha blitt lurt av en tredjeperson.[46] Ansvarsbegrensningene i § 4-30 kommer da ikke anvendelse.[47]

En ikke godkjent betalingstransaksjon forstås på denne bakgrunn som en handling som utgjør en innbetaling, overføring eller uttak av betalingsmidler etter § 1-5 sjette ledd, og som betaleren ikke har samtykket til etter § 4-2 annet ledd.

2.3 Forholdet til § 4-23 og kundens plikter

2.3.1 Innledning

Dersom en betalingstransaksjon ikke er godkjent av kunden, blir vurderingen hvordan ansvaret skal fordeles mellom kunden og betalingstjenesteyteren. Utenom kundens objektive egenandel etter § 4-30 annet ledd, beror den nærmere ansvarsfordelingen på om kunden har utvist en grov uaktsom eller forsettlig pliktforsømmelse, jf. § 4-30 tredje og fjerde ledd. Kundens plikter følger av § 4-23, og er knyttet til utstedelse og bruk av et «betalingsinstrument». Bestemmelsen gjennomfører PSD 2 artikkel 69 og er med enkelte endringer en videreføring av gjeldende rett.[48] Hva som utgjør et betalingsinstrument vil bli redegjort for i punkt 2.3.2, før kundens plikter for utstedelse og bruk behandles i punkt 2.3.3.

2.3.2 Vilkår om bruk av «betalingsinstrument»

Lovens ansvarsbegrensninger er betinget av at et «betalingsinstrument» er brukt. For avhandlingens tema er det verken hensiktsmessig eller nødvendig å avklare hva som på generelt grunnlag utgjør et betalingsinstrument. De utvalgte typetilfellene av misbruk som det vil bli redegjort for i denne avhandlingen innebærer misbruk av enten et fysisk betalingskort eller BankID for å gjennomføre transaksjoner fra nettbanken. Spørsmålet er dermed om *disse* instrumentene utgjør betalingsinstrumenter.

---

[44] Tilsvarende PSD 2 artikkel 88.

[45] Kjørven (2020) s. 91.

[46] Kjørven (2020) s. 90.

[47] Se eksempelvis BKN-2010-151, hvor en betalingstransaksjon ble ansett som godkjent til tross for at en faktura fra en håndverker var blitt forfalsket. Banken kunne ikke klandres for å ikke ha kontrollert om angitt betalingsmottaker på fakturaen samsvarte med det oppgitte kontonummeret.

[48] Prop. 92. LS (2019-2020) s. 380.

Bruk av «betalingsinstrument» har funnet sted når et «betalingsoppdrag» er iverksatt ved bruk av en «personlig innretning» eller «et sett av fremgangsmåter som er avtalt mellom kunden og betalingstjenesteyteren», jf. § 1-5 annet ledd.[49] Med «betalingsoppdrag» menes «en anmodning fra en betaler eller betalingsmottaker til en betalingstjenesteyter om å foreta en betalingstransaksjon», jf. § 1-5 femte ledd. Loven oppstiller dermed to alternative vilkår for hva som utgjør et «betalingsinstrument» når et betalingsoppdrag er iverksatt. Det første er at det må være en «personlig innretning». Ordlyden tilsier at det må være tale om en fysisk gjenstand som kun kunden kan bruke. Andre alternativ er at betalingsoppdraget må være iverksatt av «et sett av fremgangsmåter som er avtalt mellom kunden og betalingstjenesteyteren». Ordlyden er vid og legger ingen begrensninger på hva slags fremgangsmåter dette kan være, så lenge disse på forhånd er avtalt.

Både forarbeidene til finansavtaleloven (2020) og finansavtaleloven (1999) forutsetter at bruk av betalingskort med tilhørende kode er omfattet av definisjonene.[50] Videre følger det uttrykkelig av EU-domstolens sak C-287/19 *DenizBank AG mod Verein für Konsumenteninformation* at bruk av betalingskort med tilhørende kode utgjør et betalingsinstrument i form av personlig innretning.[51] Det er dermed på det rene at bruk av betalingskort til å gjennomføre en betalingstransaksjon utgjør bruk av et «betalingsinstrument», jf. § 1-5 annet ledd.

Mindre klart er det om BankID er et betalingsinstrument, ettersom bruksområdet spenner videre enn de finansielle tjenestene. Forarbeidene slår ikke fast at BankID i seg selv er et betalingsinstrument, men når BankID gjennom elektronisk autentisering brukes for å iverksette betalingssansaksjoner gjennom nettbanken, vil disse prosedyrene som må følges samlet utgjøre bruk av et betalingsinstrument.[52] EU-domstolen konkluderte tilsvarende i sak C-616/11 *T-mobile Austria GmBH mod Veren für Konsumenteninformation,* som gjaldt spørsmålet om en østerriksk mobiloperatør kunne pålegge kundene en avgift ved betaling gjennom nettbank. Betalingene ble gjennomført ved bruk av «forskellige personaliserede koder», og domstolen uttalte at «en udstedelse af en overførselsordre via netbank [udgør] et sæt af procedurer, der er aftalt mellem brugeren og udbyderen af betalingstjenester, og som brugeren bruger for at initiere en betalingsordre».[53]

[49] Tilsvarende PSD 2 artikkel 4 nr. 14.

[50] Prop. 92 LS (2019-2020) s. 117 og Ot.prp.nr. 94 (2008-2009) s. 171.

[51] Sak 287/19 *DenizBank* avsnitt 70 og 73.

[52] Prop 92. LS (2019-2020) s. 175.

[53] C-616/11 *T-mobile Austria* avsnitt 41 og 42.

Forholdet er parallelt med hvordan BankID i Norge benyttes til å gjennomføre transaksjoner i nettbanken. Kunden logger seg inn med personnummer, engangskode og passord og kan gjennomføre betalingsoppdrag etter samme prosedyre. Dette utgjør følgelig et «sett av fremgangsmåter» som er forhåndsavtalt mellom kunden og betalingstjenesteyteren for å gjennomføre et betalingsoppdrag. Det samme legges til grunn av Høyesterett uten nærmere begrunnelse i HR-2020-2021-A avsnitt 38.

Dermed omfattes både bruk av fysisk betalingskort og bruk av BankID til å iverksette et betalingsoppdrag av definisjonen av «betalingsinstrument» i 1-5 annet ledd, og uautorisert bruk av disse vil utgjøre en ikke godkjent betalingstransaksjon etter § 4-30.

2.3.3 Kundens plikter ved utstedelse og bruk av betalingsinstrument

Utgangspunktet for skyldvurderingen er kundens plikter etter § 4-23, jf. § 4-30. Bestemmelsen tilsvarer finansavtaleloven (1999) § 34 og gjennomfører PSD 2 artikkel 69. Etter § 4-23 pålegges kunden å bruke betalingsinstrumentet i samsvar med «vilkårene for utstedelse og bruk» og må «ta alle rimelige forholdsregler» for å beskytte «personlig sikkerhetsinformasjon». Med «personlig sikkerhetsinformasjon» siktes det til «personaliserte innretninger som en tjenesteyter stiller til rådighet for kunde eller annen bruker for autentiseringsformål», jf. § 1-8 tiende ledd.[54] Dette omfatter eksempelvis PIN-kode eller annet passord for å bekrefte iverksettelsen av en betalingstransaksjon.[55] I tillegg er kunden pålagt en varslingsplikt etter § 4-24.

Kundens plikter følger nærmere av utstedelsesavtalen. Betalingstjenesteyteren står ikke fritt til å styre kundens forpliktelser gjennom en streng avtaleregulering, ettersom loven er ufravikelig til ugunst for forbrukeren, jf. § 1-9. I § 4-23 første ledd presiseres det at «[v]ilkårene for utstedelse og bruk skal være objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet». Dette utgjør preseptoriske «normalregler», som setter grenser for betalingstjenesteyters mulighet til å avtale seg ut av et eventuelt ansvar.[56] Det nærmere innholdet i utstedelsesavtalen beror på en konkret tolkning, hvor utgangspunktet er en objektiv forståelse av avtalens ordlyd.[57]

Forbrukeravtaledirektivet stiller krav til avtalens innhold i forbrukerforhold.[58] Artikkel 5 slår fast at avtalevilkårene skal formuleres på en «klar og forståelig måte». EU-domstolen har slått

[54] Tilsvarende PSD 2 artikkel 4 nr. 31.

[55] Prop. 92 LS (2019-2020) s. 168.

[56] Woxholth (2017) s. 450.

[57] Eksempelvis HR-2020-1262-A avsnitt 43.

[58] Rådsdirektiv 93/13/EØF av 5. april 1993.

fast at det i dette ligger mer enn at avtalens innhold skal være grammatisk riktig utformet.[59] Det er for det første tale om en objektiv klarhetsstandard, hvor det sentrale er hva en alminnelig opplyst og rimelig oppmerksom forbruker ville ha forstått.[60] For det andre pålegges næringsdrivende en forklaringsplikt, hvor forbrukeren må opplyses om avtalevilkårene og konsekvensene av disse før avtalen inngås.[61] Dette vil supplere betalingstjenesteyters opplysningsplikt etter finansavtaleloven (2020) § 3-31, og vil være en viktig tolkningsfaktor ved tolkningen av utstedelsesavtalen.

Plikten til å beskytte sikkerhetsinformasjon følger av lovens krav om at kunden må ta «alle rimelige forholdsregler», jf. § 4-23. At sikkerhetsinformasjonen skal være «personlig», tilsier at ingen andre skal ha tilgang til denne. At forholdsreglene skal være «rimelige», innebærer en øvre grense for hvor inngripende forholdsregler det kan forventes at kunden iverksetter. I HR-2020-2021-A, som gjaldt misbruk av BankID til opptak av forbrukslån, uttalte retten seg om hva som ligger i «rimelige forholdsregler» etter finansavtaleloven (1999) § 34 i avsnitt 98: «Vurderingen av hva som er rimelige forholdsregler, må bygge på hva som praktisk mulig uten at det utgjør en urimelig stor byrde for innehaveren eller vil gjøre selve bruken av BankID upraktisk». Det forventes følgelig ikke at kunden treffer tiltak som går utover den praktiske nytten av å inneha betalingsinstrumentet.[62]

Hva som utgjør rimelige forholdsregler, må vurderes med utgangspunkt i hvordan betalingsinstrumentet brukes og oppbevares. Dersom betalingsinstrumentet oppbevares nedlåst i en koffert, så har ikke kunden tatt alle rimelige forholdsregler dersom tilhørende kode eller passord er nedtegnet og oppbevares samme sted.[63] Det er altså nærliggende å forstå kravet om at betalingsinstrumentet skal brukes «i samsvar med vilkårene for utstedelse og bruk» og kravet om «rimelige forholdsregler» i relasjon til hverandre, der kundens plikter er situasjonsavhengig. Kunden holdes imidlertid ikke ansvarlig for ethvert avvik fra disse pliktene. Det kreves at kunden har utvist grov uaktsomhet eller forsett, som vil bli nærmere redegjort for i kapittel 3 og 4.

[59] C-26/13 *Kásler og Rábai mod OTP Jelzálogbank Zrt.* avsnitt 71.
[60] C-26/13 *Kásler og Rábai mod OTP Jelzálogbank Zrt.* avsnitt 74.
[61] C-186/16 *Andriciuc m.fl. mod Banca Românească SA* avsnitt 47.
[62] Grøttjord og Rosén (2014) s. 205.
[63] Slik som i Rt. 2004 s. 499, se nærmere i punkt 3.3.

3 Terskelen for grovt uaktsomme pliktbrudd

3.1 Innledning

Finansavtaleloven § 4-30 tredje ledd slår fast at ansvaret begrenses til 12 000 kroner dersom kundens betalingsinstrument er brukt til å gjennomføre en ikke godkjent betalingstransaksjon. I dette kapittelet vil det nærmere redegjøres for hva som ligger i uttrykket «grov uaktsomhet» og hva som skal til for å konstatere grovt uaktsomme pliktbrudd etter finansavtaleloven (2020) § 4-30. I punkt 3.2 og 3.3 vil det redegjøres for aktsomhetsbegrepet i finansavtaleloven generelt og i lys av høyesterettspraksis. I punkt 3.4 vil spørsmålet om betydningen av kundens subjektive forhold nærmere behandles. Dette punktet vil også være relevant for de forsettlige pliktbruddene, men behandles av hensyn til avhandlingens fremstilling under kapittel 3. I punkt 3.5 vil det redegjøres for utvalgte typetilfeller hvor grov uaktsomhet vil være aktuelt, før kapittelet sammenfattes i punkt 3.6.

3.2 Om aktsomhetsbegrepet i finansavtaleloven

Finansavtaleloven definerer ikke uttrykket «grov uaktsomhet». Ordlyden tilsier at det er tale om en høy terskel, slik at bestemmelsen er reservert for de mest alvorlige tilfellene av pliktforsømmelser begrenset oppad mot forsett. Av fortalen til PSD 2 punkt 72 følger det at «[s]elv om begrebet forsømmelse indebærer tilsidesættelse af diligenspligten, bør grov forsømmelse imidlertid indebære mere end blot forsømmelse og vedrøre adfærd, der involverer en betydelig grad af skødesløshed [...]». For det første vil altså ikke enhver pliktforsømmelse omfattes av bestemmelsen, det må nemlig være tale om et kvalifisert avvik.[64] For det andre presiserer direktivet at pliktforsømmelsen må innebære en betydelig grad av uforsiktighet. Som eksempel trekkes frem «opbevaring af de sikkerhedsoplysninger, der anvendes til at give tilladelse til en betalingstransaktion, ved siden af betalingsinstrumentet i et format, der på en åben og let måde kan opdages af tredjeparter». Typisk vil dette omfatte oppbevaring av nedskrevet kode sammen med bankkortet i en lommebok.

I nevnte HR-2020-2021-A uttalte Høyesterett seg om ikke godkjente betalingstransaksjoner etter finansavtaleloven (1999) § 35 i et obiter dictum:[65]

> «Når BankID benyttes innenfor det som må betegnes som det opprinnelige bruksområdet, betalingstransaksjoner, må den klare hovedregelen være at det ikke kan kreves at institusjonen skal foreta ytterligere sikkerhets- eller kontrolltiltak utover å konstatere at BankID er brukt på riktig måte. Dette må da danne utgangspunktet for

[64] Slik også forarbeidene til finansavtaleloven (1999) forutsetter: «[f]or at kunden skal anses å ha vært grovt uaktsom, kreves det imidlertid et markert avvik fra vanlig forsvarlig handlemåte», jf. Ot.prp.nr. 94 (2008-2009) s. 117.

[65] HR-2020-2021-A avsnitt 58.

vurderingen av om innehaveren har opptrådt grovt uaktsomt etter finansavtaleloven § 35 tredje ledd.»

Dette må leses i sammenheng med at betalingstjenesteyteren selv tilhører en gruppe som forventes å iverksette tiltak for å unngå at tap oppstår, noe som kan påvirke skyldvurderingen.[66] Uttalelsen kan tas til inntekt for at det er tilstrekkelig for betalingstjenesteyteren å godtgjøre at BankID er brukt riktig. Skyldvurderingen beror da på en isolert vurdering av hva *kunden* kunne og burde ha gjort, mens dette ikke nødvendigvis er situasjonen der BankID brukes i andre sammenhenger.[67]

Ettersom saken gjaldt skyldreglene etter finansavtaleloven (1999), behandlet ikke Høyesterett PSD 2, som i fortalen punkt 72 uttrykkelig slår fast at «[f]or at vurdere eventuel forsømmelse eller grov forsømmelse fra betalingstjenestebrugerens side bør der *tages hensyn til alle omstændigheder*» (min utheving). Det vil si at dersom betalingstjenesteyteren kan iverksette tiltak for å forbedre sikkerheten utover selve bruken av BankID, må dette hensyntas i skyldvurderingen. Videre følger det av teknisk standard til PSD 2, som supplerer direktivet, at betalingstjenesteytere plikter å ha «transaktionsovervågningsmekanismer, som sætter dem i stand til at afsløre uautoriserede eller svigagtige betalingstransaktioner».[68] Det skal altså være rutiner på plass for å avdekke svindel og misbruk av betalingsinstrumenter. Mangel på slike rutiner vil antagelig måtte ha betydning for skyldvurderingen ved kundens pliktbrudd.

Det finnes ikke autorativ EU- eller EØS-rettslig praksis knyttet til vurderingen av grov uaktsomhet. Høyesterett har kun ved ett tilfelle, i Rt. 2004 s. 499, vurdert terskelen for grovt uaktsomme pliktbrudd ved ikke godkjente betalingstransaksjoner. Avgjørelsen gjaldt finansavtaleloven (1999) § 35 før implementeringen av PSD 1, hvor kundens ansvar var begrenset til en egenandel dersom kunden grovt uaktsomt hadde «muliggjort misbruket». Selv om skyldansvaret etter denne bestemmelsen ikke knytter seg til kundens plikter, er Høyesteretts uttalelser om skyldkravet av sentral betydning også for finansavtaleloven (2020).

3.3 Grov uaktsomhet i lys av Rt. 2004 s. 499.

Spørsmålet i Rt. 2004 s. 499 var om innehaveren av et kredittkort ved grov uaktsomhet hadde muliggjort en tredjepersons misbruk av kortet. Høyesterett delte seg i tre mot to, hvor flertallet konkluderte med at kunden ikke hadde opptrådt grovt uaktsomt.

[66] HR-2020-2021-A avsnitt 61.

[67] HR-2020-2021-A avsnitt 59.

[68] Forordning (EU) 2018/389 artikkel 2 nr. 1.

Saken gjaldt en kunde som hadde tre bankkort låst i en koffert i en låst leilighet i Spania. Kodene var skrevet ned i kamuflert form i en almanakk, som ble oppbevart i samme koffert. Kamufleringen besto av en kombinasjon av åtte sifre på tre rekker, hvor de fire første sifrene i hver rekke var fødselsdatoen til hvert av kundens tre barn og de fire siste var koden til hvert bankkort. Øverst på samme side var forbokstaven til hvert av barna knyttet til hvert av bankkortene. En innbruddstyv hadde brutt seg inn i leiligheten og stjålet kortene. For kortet som ble misbrukt, et MasterCard med koden 1275, var koden kamuflert slik: F/M (øverst på siden) 30041275 (nederst på siden).

Aktsomhetsvurderingen knyttet seg til to forhold, nemlig nedskrivingen av kodene og oppbevaringen av kortene og kodene.[69] På den tiden fremgikk det uttrykkelig av avtalevilkårene at «PIN-koden må ikke noteres», som betalingstjenesteyteren mente etablerte handlingsnormen som dannet grunnlaget for skyldvurderingen.[70] I et tilhørende skriv sto det imidlertid at «[k]oden må ikke noteres i noen form slik at andre kan finne ut av hva tallene gjelder». Mindretallet mente at skrivet var en begrunnelse for hvorfor koden ikke måtte nedtegnes.[71] Flertallet mente imidlertid at skrivet var egnet til å gi inntrykk av at det sentrale var at andre ikke skulle kunne finne frem til tallene.[72] Begrunnelsen var at det ville være «meget vanskelig» å praktisere en ordning hvor koden aldri kunne nedtegnes. Kunden hadde et berettiget behov for å skrive ned kodene, og flertallet fant det klart at det å notere koden ikke i seg selv var grovt uaktsomt.[73] Mindretallet konstaterte imidlertid at det her forelå et avtalebrudd, men presiserte at dette ikke var tilstrekkelig for å konstatere grov uaktsomhet.[74] Både flertallet og mindretallet var da enige i at det ved skyldvurderingen måtte tas utgangspunkt i en samlet bedømmelse av situasjonen.

Ved tolkningen av uttrykket «grov uaktsomhet» slo flertallet fast at kunden må ha utvist en kvalifisert form for uaktsomhet.[75] Flertallet uttalte at en grov uaktsom oppførsel 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». Forarbeidene understøttet dette, og flertallet avviste ankemotpartens påstand om at det var avtalen som etablerte handlingsnormen. Mindretallet var på dette punkt enig.[76]

[69] Rt. 2004 s. 499 avsnitt 27.
[70] Rt. 2004 s. 499 avsnitt 28.
[71] Rt. 2004 s. 499 avsnitt 49.
[72] Rt. 2004 s. 499 avsnitt 29.
[73] Rt. 2004 s. 499 avsnitt 31.
[74] Rt. 2004 s. 499 avsnitt 50.
[75] Rt. 2004 s. 499 avsnitt 32.
[76] Rt. 2004 s. 499 avsnitt 48.

Høyesterett fastla dermed vurderingstemaet for grov uaktsomhet. Det ble lagt opp til en toleddet aktsomhetsvurdering, tilsvarende den i erstatningsretten.[77] Det må for det første foreligge et *objektivt avvik* fra en vanlig forsvarlig handlenorm. Det følger av flertallets videre drøftelse at målestokken er den «alminnelige kortholder».[78] Standarden er med andre ord ikke idealkunden. Dette objektive avviket må være «markert», som innebærer at ikke ethvert avvik fra den alminnelige handlenormen vil omfattes.[79] For det andre vurderes det om det foreligger en *subjektiv unnskyldningsgrunn*. Kundens opptreden må være «sterkt klanderverdig», slik at det må foreligge et element av bebreidelse hvor kunden må være «vesentlig mer å klandre».

I den konkrete vurderingen var det sentralt om koden var notert slik at det muliggjorde en tredjepersons misbruk av kortet.[80] Flertallet slo fast at «folk flest» antakelig ville hatt vanskeligheter med å finne riktig kode.[81] Samtidig fremhevet flertallet at en profesjonell svindler kan ha gode ferdigheter i å avsløre kamuflerte koder, og selv om det ikke kunne stilles krav til at kunden hadde innsikt i slike metoder, så var dette «likevel noe man må ta hensyn til». Flertallet påpekte at kunden hadde andre handlingsalternativer i form av at kamufleringen kunne vært bedre. Flertallet mente derfor at kunden kunne bebreides for ikke å ha kamuflert koden godt nok og at dette isolert sett var uaktsomt.[82]

Det slås dermed fast at kunden ikke har opptrådt slik en alminnelig aktsom kunde ville ha gjort, og kunden kunne bebreides for dette. Hvorvidt det i det hele tatt foreligger uaktsomhet, vil ut fra uttalelsene bero på en vurdering av hvor godt koden er kamuflert, herunder om den er kamuflert slik at «folk flest» ikke vil finne frem til koden.

Samtidig må kunden ta hensyn til at det finnes profesjonelle svindlere, som tilsier at Høyesterett mener at koden ikke bare skal kamufleres for «folk flest». Det er noe uklart hva Høyesterett sikter til, men den mest nærliggende er at kunden bør unngå de mest opplagte formene for kamuflering. Det etableres en sikkerhetsventil for de tilfellene kunden har valgt en kamufleringsmetode som eksempelvis har blitt advart mot i offentligheten. Uttalelsene kan imidlertid vanskelig forstås slik at kamufleringen skal være umulig å avdekke av profesjonelle svindlere. Dette ville i praksis betydd et objektivt ansvar for en høyere egenandel i de tilfellene kunden har skrevet ned passordet i kamuflert form, men betalingsinstrumentet likevel blir misbrukt.

---

[77] Kjelland (2020) s. 69 og 96.

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

[79] Sml. fortalen til PSD 2 punkt 72.

[80] Rt. 2004 s. 499 avsnitt 33.

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

[82] Rt. 2004 s. 499 avsnitt 37.

Høyesterett trekker frem to sentrale forhold ved vurderingen av om uaktsomheten kunne kategoriseres som grov, nemlig at koden kunne vært kamuflert bedre og at kunden betydelig kunne redusert risikoen for svindel ved å medbringe notatboken. Det sentrale i skyldvurderingen er altså kundens *handlingsalternativer*, hvor det var «ubetenksomt» å la kort og kode ligge sammen, til tross for at disse var nedlåst i en koffert i en forsvarlig låst leilighet som ikke var spesielt utsatt for innbrudd.[83] Uttalelsene tilsier at kort og kode ikke bør oppbevares sammen i det hele tatt, og terskelen for grov uaktsomhet kan tenkes å være nokså lav i disse tilfellene.

Høyesterett anså imidlertid ikke kundens handlinger som «sterkt klanderverdige», og kunden hadde følgelig ikke opptrådt grovt uaktsomt. Dette ble begrunnet med at oppbevaringen hadde et «klart midlertidig preg», men flertallet påpekte samtidig at vurderingen ville blitt en annen om kunden oppbevarte kort og kode i nærheten av hverandre i sitt eget hjem. Oppbevaringens midlertidige karakter og det forhold at kunden var på ferie var altså utslagsgivende momenter. Det impliseres altså at risikoen for misbruk er mindre der kort og kode midlertidig oppbevares sammen enn om de oppbevares slik varig i eget hjem.

Avslutningsvis påpeker flertallet at håndteringen av kort og kode må gis en «streng aktsomhetsvurdering». Dette forklares ikke nærmere, men ut fra sammenhengen er det mest nærliggende at aktsomhetskravet skjerpes ved håndteringen av betalingsinstrumenter og tilhørende koder og passord. Det er imidlertid uklart hvordan dette skal forstås i lys av vurderingstemaet om at det må være et «markert avvik» fra vanlig forsvarlig handlemåte hvor kunden er «vesentlig å bebreide». En viss veiledning følger av de videre uttalelsene om at det «spiller likevel inn at det økonomiske tap [...] var begrenset til kr 10.000».[84] Høyesterett kommenterer altså *skadeevnen*, hvor kombinasjonen av oppbevaringens midlertidige karakter og at det økonomiske tapet var begrenset, medførte at skadeevnen var relativt liten. Lest i sammenheng med at det ifølge Høyesterett forelå flere handlingsalternativer som betydelig kunne redusert tapsrisikoen, forstås uttalelsene slik at kombinasjonen av skaderisikoen og kundens mulighet til å redusere denne gjennom ulike handlingsalternativer vil utgjøre kjernen i vurderingen av grov uaktsomhet. Hvor «streng» aktsomhetsnorm som skal legges til grunn er med andre ord relativ til skadeevnen i det enkelte tilfellet.

En slik forståelse innebærer at en kunde med betydelige midler må utvise en større grad av aktsomhet enn en kunde med lite midler. Videre vil BankID måtte stå i en særstilling, ettersom det potensielle økonomiske tapet i teorien er ubegrenset. Dette har sine åpenbare begrensninger,

[83] Rt. 2004 s. 499 avsnitt 38 og 39.

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

ettersom det skaper en høyst uforutsigbar stilling i avtaleforholdet med betalingstjenesteyteren. Nettopp hensynet til forutsigbarhet er sentralt i kontraktsretten og vil tillegges betydelig vekt i favør forbrukeren ved en eventuell tvist.[85] Kunden påtar seg ikke en større tapsrisiko kun fordi vedkommende har mer midler, og aktsomhetsvurderingen må i det vesentlige bero på om det er utvist «et markert avvik fra vanlig forsvarlig handlemåte» hvor det det må dreie seg om «en opptreden som er sterkt klanderverdig». Skadeevnen vil til en viss grad kunne være veiledende i denne vurderingen, men etablerer ikke i seg selv handlenormen.

Mindretallet kom til et annet resultat og baserte vurderingen på en sannsynlighetsbedømmelse. Tyven kunne for hvert kort begynne med de første fire sifrene på øverste tallrekke og jobbe seg fremover. Hvis det første kortet ble sperret etter å ha uttømt de øverste to tallrekkene, kunne tyven vite at koden for dette kortet skjulte seg i siste tallrekke. Tyven ville da treffe riktig kode til begge de to neste kortene om han fulgte samme systematikk.[86] Det avgjørende ble da at kodene ikke var godt nok kamuflert og kunden «meget enkelt» kunne redusert muligheten for misbruk.[87] Dette hvilte imidlertid på to sentrale forutsetninger: For det første måtte tyven forstå at disse sifrene skjulte kodene til de aktuelle kortene.[88] Dette er ut fra opplysningene i saken ikke gitt, da de isolert sett fremsto som frittstående tallrekker uten noen nærmere sammenheng. Tyven hadde heller ingen forutsetninger til å koble fødselsdagen til kundens barn med det enkelte kort. For det andre måtte tyven forstå at det enten var de fire første eller fire siste sifrene som var koden, og ikke en hvilken som helst annen kombinasjon.[89]

Oppsummert så avklarte Høyesterett vurderingstemaet for grov uaktsomhet, hvor det sentrale er at det må foreligge 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».[90] Skyldvurderingen beror på en samlet bedømmelse av forholdene i den individuelle saken, hvor sentrale momenter vil være skadeevnen og kundens handlingsalternativer.

Misbruk av elektroniske betalingsinstrumenter kan skje på en rekke ulike måter som i større eller mindre grad ligner forholdene i denne dommen. Spørsmålet blir dermed hvordan vurderingen av grov uaktsomhet skal løses i andre tilfeller av misbruk. Dette vil behandles nærmere under punkt 3.5. Før dette, vil spørsmålet om hvilken betydning kundens subjektive forhold har for skyldvurderingen behandles i punkt 3.4.

[85] Giertsen (2019) s. 8.

[86] Rt. 2004 s. 499 avsnitt 54.

[87] Rt. 2004 s. 499 avsnitt 56 og 57.

[88] Rt. 2004 s. 499 avsnitt 52.

[89] Rt. 2004 s. 499 avsnitt 53.

[90] Slik som i kontraktsretten ellers, se Hagstrøm (2011) s. 483.

3.4 Betydningen kundens individuelle forhold

Om kunden lar seg lure av ulike svindelmetoder vil i mange tilfeller bero på personlige forutsetninger. Kundens prøves imidlertid etter en objektiv norm, «den alminnelige kortholder» eller mer generelt «den alminnelige bankkunde». Det er samtidig klart at individuelle forutsetninger vektlegges i både erstatningsretten og kontraktsretten, hvor profesjonsansvaret er det tydeligste eksempelet på dette.[91] I erstatningsretten kan subjektive forhold være avgjørende for aktsomhetsvurderingen, der det eksempelvis stilles lempeligere krav til barn enn til voksne.[92] Mindre åpenbart er det om andre forhold også kan vektlegges, slik som kundens høye alder eller manglende språkkunnskap.

Kundens *høye alder* kan etter omstendighetene medføre at vedkommende ikke har de samme forutsetningene som befolkningen for øvrig til å avdekke svindelforsøk. Som en konsekvens av den digitale utviklingen er det en kjensgjerning at det har oppstått et kunnskapsgap mellom yngre og eldre generasjoner med hensyn til teknologi og bruk av digitale løsninger. Analoge bankkunder har i stadig mindre grad mulighet til å benytte seg av tradisjonelle betalingstjenester og mange finner det krevende å bruke elektroniske betalingsløsninger på egenhånd. Disse kundene søker gjerne hjelp hos familie og venner, som innebærer at det oppstår en større risiko for svindel.[93] Svindlere utnytter gjerne denne mangelen på digital kunnskap, som eksempelvis vises gjennom sakene om såkalt «Olga-svindel» hvor svindlere målrettet kontakter eldre mennesker.

Innenfor erstatningsrettslig teori hevdes det at høy alder i kombinasjon med alderdomssvekkelser kan føre til en mildere aktsomhetsbedømmelse.[94] Dette er forhold som kan ha innvirkning på en persons evne til å oppfatte risiko og vurdere aktuelle handlingsalternativer, slik at det kan medføre en lempeligere aktsomhetsvurdering. Dette er imidlertid omdiskutert.[95] I forarbeidene til finansavtaleloven (2020) forutsettes det i tilknytning til vurderingen av forsettlige pliktbrudd at «eldre personer [...] som har behov for hjelp av andre til å betale regninger» ikke uten videre skal være ansvarlige for hele det økonomiske tapet.[96] Forarbeidene impliserer med dette at kundens høye alder etter omstendighetene vil være et relevant moment i skyldvurderingen. En slik løsning har gode grunner for seg, nettopp fordi manglende kunnskap om bruk og risiko innebærer at disse gruppene i større grad er utsatt for svindel.

---

[91] Hagstrøm (2011) s. 468 og Hagstrøm og Stenvik (2019) s. 169.

[92] Hagstrøm og Stenvik (2019) s. 171.

[93] Finanstilsynet (2020) s. 42.

[94] Hagstrøm og Stenvik (2019) s. 172.

[95] Kjelland (2019) s. 94-95.

[96] Innst. L (2020-2021) s. 22.

Også *manglende språkkunnskap* kan være aktuelt å tillegge en viss vekt. Å stille samme krav til flyktninger og asylsøkere, eller andre som nylig har flyttet til Norge fra et annet land og fra en annen kultur, kan etter omstendighetene fremstå urimelig. Disse kundene har ikke de samme språklige forutsetningene som befolkningen for øvrig til å sette seg inn i og forstå den risiko elektroniske betalingsløsninger medfører.

Problemstillingen har blitt behandlet av lagmannsretten i LB-2016-43622 etter gjeldende finansavtalelov. Saken gjaldt en kvinne som på grunn av begrensede norskkunnskaper overlot BankID og passord til sin ektefelle, som senere misbrukte dette til å ta opp lån uten at kunden var klar over hva hun signerte på. Saken gjaldt altså misbruk av elektronisk signatur, men det uttales på generelt grunnlag at «[m]anglende kunnskap i norsk og om det norske banksystemet burde føre til at hun var mer forsiktig med å undertegne på dokumenter som hun ikke forsto innholdet i». Kundens manglende språkkunnskap ble ikke tillagt vekt, og lagmannsretten anså det som uaktsomt av kunden å undertegne en avtale uten å sette seg inn i hva vedkommende forpliktet seg til.

Dette vil imidlertid harmonere dårlig med betalingstjenesteyterens opplysnings- og forklaringsplikt, jf. over i punkt 2.3.3. Utgangspunktet er at det er betalingstjenesteyteren som skal sørge for at kunden har fått tilstrekkelig kunnskap om bruk og risiko av betalingsinstrumentet. Dette vil i enda større grad gjelde der kunden ikke har tilstrekkelig språkkunnskaper til selv å sette seg inn i dette. Videre følger det av forarbeidene til finansavtaleloven (2020) at kunder som har behov for hjelp på grunn av manglende språkkunnskap ikke uten videre kan holdes ansvarlige for forsettlige pliktbrudd.[97] Med dette legger forarbeidene til grunn at manglende språkkunnskaper er et relevant individuelt forhold i skyldvurderingen.

Også andre subjektive forhold kan være aktuelle å se hen til, eksempelvis lettere psykisk utviklingshemming,[98] eller kundens utdanningsnivå. Det vil imidlertid være for omfattende å diskutere alle relevante subjektive forhold som kan ha betydning for skyldvurderingen. Det vesentlige er at forarbeidene uttrykkelig nevner alder og språkkunnskap som relevante subjektive forhold, og dermed åpner for at subjektive forhold er relevante ved skyldvurderingen. Et slikt standpunkt er også inntatt i forarbeidene til finansavtaleloven (1999), som fremhever at krav til forsiktighet og egenkontroll varierer fra kunde til kunde, slik at det er «viktig å vurdere kundens kunnskap og innsikt i den enkelte betalingstjeneste».[99]

[97] Innst. L (2020-2021) s. 22.

[98] Eksempelvis BKN-2008-81.

[99] NOU 2008:21 s 105.

3.5 Grov uaktsomhet i utvalgte typetilfeller av ikke godkjente betalingstransaksjoner

3.5.1 PIN-kode og betalingsinstrument misbrukes av tredjeperson

Det vil her redegjøres nærmere for situasjoner som etter sin art ligner på saksforholdet i Rt. 2004 s. 499, nemlig der en tredjeperson tilegner seg kundens betalingsinstrument og sikkerhetsinformasjon. Spørsmålet er hvor grensen for grovt uaktsomme pliktbrudd skal trekkes ved ulike situasjoner der en tredjeperson har fått tilgang til kundens kode og betalingsinstrument. Aktsomhetsvurderingen vil på bakgrunn av Høyesteretts avgjørelse bero på oppbevaringen av betalingsinstrumentet og eventuelt kamufleringen av koden. Dette er fulgt opp av praksis fra Finansklagenemnda, hvor det gjennomgående slås fast at kunden har opptrådt grovt uaktsomt dersom koden har blitt oppbevart sammen med kortet i åpen eller i dårlig kamuflert form.[100]

Oppbevares koden *adskilt* fra betalingsinstrumentet, vil vurderingen også her bero på et samspill av hvor godt koden er kamuflert og oppbevaringen. Samtidig innebærer situasjonen i seg selv at risikoen for misbruk blir betraktelig mindre, da svindleren må finne ut av oppbevaringsstedet for både betalingsinstrumentet og den tilhørende koden. Dette tillater at oppbevaringen kan være av mer varig karakter. Følgelig skal det mer til for at kunden i slike situasjoner har opptrådt grovt uaktsomt. Dersom det er truffet gode sikkerhetstiltak ved oppbevaringen av selve koden, vil det også måtte stilles lempeligere krav til kvaliteten på kamufleringen.

Finansklagenemnda har i flere saker konkludert at det er tillatt å oppbevare koden i hjemmet, eksempelvis i FinKN-2013-276 hvor en innbruddstyv hadde stjålet kundes bankkort og nedskrevne kode mens kunden var hjemme. Nemnda kom til at det var ikke grovt uaktsomt å oppbevare kort og kode i eget hjem, selv om koden var notert i klartekst. Nemnda presiserte at tapsrisikoen er betydelig redusert der innbruddet skjer mens kunden oppholder seg hjemme. At det skal gå et skille mellom tilfellene der kunden oppholder seg hjemme eller ikke under et innbrudd vil umiddelbart virke kunstig. Det avgjørende for aktsomhetsvurderingen er ikke hvor kortholder oppholder seg når innbruddet skjer, men hvordan kort og kode er oppbevart. Det er ikke et krav at kunden til enhver tid skal ha betalingsinstrumentet med seg. I FinKN-2014-528 kom nemnda til motsatt resultat. Kunden oppbevarte bankkortet i lommeboken mens den ukamuflerte koden lå i en hylle i leiligheten. Kunden hadde latt besøk oppholde seg alene i leiligheten, som senere misbrukte bankkortet. Slik oppbevaring utgjorde etter nemndas syn et grovt uaktsomt pliktbrudd, ettersom kort og kode var «lett tilgjengelig for den fremmede mannen som oppholdt seg alene i boligen».

[100] Eksempelvis FinKN-2020-230, FinKN-2020-52 og FinKN 2017-580.

Det vil med andre ord etter omstendighetene måtte stilles strengere krav til hvordan kort og kode oppbevares dersom man lar utenforstående tredjepersoner oppholde seg i hjemmet uten at det treffes ytterligere sikkerhetstiltak. I slike tilfeller skaper kunden en situasjon hvor risikoen for at skadepotensialet realiserer seg blir betydelig større. Til dette kan det innvendes at sannsynligheten for et slikt tillitsbrudd fra bekjente vil skje må antas å være minimal, med mindre det foreligger konkrete omstendigheter som tilsier noe annet. Det er ikke slik at kunden må være skeptisk til sine gjesters intensjoner, samtidig må det forventes at kunden tar visse forholdsregler – eksempelvis ved at koden kamufleres eller at kunden ikke oppbevarer kort og kode i nærheten av hverandre når andre har tilgang til hjemmet. Dersom besøket oppholder seg alene, og kort og kode ligger åpent tilgjengelig, vil dette etter omstendighetene kunne utgjøre et grovt uaktsomt pliktbrudd.

Et særlig spørsmål oppstår i de tilfellene det er kundens nærstående som misbruker betalingsinstrumentet. Ektefeller, samboere og barn har naturlig nok enklere tilgang til kundens betalingsinstrumenter, og kundens handlingsalternativer er mer begrenset enn når det er tale om en utenforstående tredjeperson. Dette er forhold som etter omstendighetene kan medføre at det stilles strengere krav til hvordan kunden bruker og oppbevarer betalingsinstrumentet og kodene. Kunden påtar seg imidlertid ikke en større tapsrisiko ved å inngå i et forhold med en annen person, og aktsomhetsvurderingen må også her ta utgangspunkt i om det foreligger konkrete omstendigheter som gir kunden oppfordring til å handle annerledes.

Saker hvor nærstående misbruker kundes betalingsinstrumenter har blitt behandlet i noen eldre avgjørelser fra daværende Bankklagenemnda. I BKN-2006-127 kom nemnda til at kunden hadde handlet grovt uaktsomt i en sak hvor kunden lot datteren disponere leiligheten mens hun selv var bortreist. Bankkort og ukamuflert kode ble oppbevart i hvert sitt rom. Nemnda uttalte «at kombinasjonen av oppbevaringen og det forhold at kortholder lot sin narkomane datter disponere leiligheten alene mens kortholder var bortreist, medførte en slik øket risiko for misbruk at forholdet samlet sett må anses som grovt uaktsomt». Saken har likhetstrekk med ovennevnte FinKN-2014-528, men nemnda går i denne saken langt i å tillegge subjektive forhold hos svindleren avgjørende vekt. Nemnda kom til motsatt resultat i BKN-2007-150, der kundens sønn urettmessig overførte penger fra morens konto til sin egen. Det var uavklart hvordan kunden oppbevarte kodebrikke og passord, men nemnda la til grunn at sønnen måtte ha kjennskap til disse. Forholdet ble ikke ansett som grovt uaktsomt ettersom sønnen hadde «utvist et forbrytersk forsett, og bedratt sin mor på en utspekulert måte», og moren kunne ikke bebreides for å ha besøk av sønnen sin. Sønnen hadde tidligere sonet to fengselsdommer for nettsvindel, men dette ble ikke tillagt vekt da svindelen ikke var rettet mot moren. Nemnda har

konkludert tilsvarende i lignende saker,[101] også i tilfeller hvor det er samboeren som har stjålet kort og kode.[102]

Avgjørelsene viser at det som utgangspunkt ikke anses grovt uaktsomt å oppbevare kort og kode i hjemmet, men at dette kan være tilfellet hvis man lar en tredjeperson oppholde seg der alene. Hvis det er tale om en nærstående eller bekjent, kan subjektive forhold ha avgjørende vekt i aktsomhetsvurderingen. Barnets tidligere bedrageridommer ble ikke tillagt vekt i en sak, mens barnets rusproblemer ble tillagt vekt i en annen sak. Hvorvidt slike forholdt er relevant i aktsomhetsvurderingen vil hovedsakelig bero på om kunden *burde* har forstått at de subjektive forholdene hos svindleren innebar en risiko, og basert på dette *skulle* ha handlet annerledes. At barnet er bedrageridømt er åpenbart en relevant omstendighet, men som nemnda rettmessig påpeker hadde ikke foreldrene grunn til å reagere ettersom denne svindelen ikke var rettet mot dem. Det er vanskelig å se hvilken årsakssammenheng det er mellom barnets rusproblemer og muligheten for at vedkommende svindler sine foreldre, og etter min oppfatning går nemnda for langt i å tillegge dette vekt i aktsomhetsvurderingen.

3.5.2 Phishing – tilfeller der kunden følger en digital lenke og oppgir sikkerhetsinformasjon

Her vil det nærmere redegjøres for hvordan kundens skyld vurderes i tilfeller der kunden har blitt utsatt for phishing. Med dette menes, som forklart innledningsvis, tilfeller der kunden blir lurt til å følge en digital lenke vedkommende har mottatt. Lenken dirigerer kunden til en side som i større eller mindre grad ligner på nettsiden til kundens bank eller en annen aktør hvor vedkommende er registrert kunde. Svindlerne har kontroll over narresiden, hvor de kan se innloggingsinformasjonen som blir tastet inn. Ved å illudere en mislykket innlogging på narresiden, kan svindlerne gjentatte ganger få nødvendig informasjon for å gjennomføre flere betalingstransaksjoner. Situasjonen er en ganske annen enn ved «tradisjonell» svindel, hvor svindleren fysisk fratar kunden betalingsinstrumentet og den tilhørende koden. Ved phishing har kunden fortsatt alt i sin besittelse, men har blitt lurt til å oppgi tilstrekkelig informasjon for at svindleren selv kan gjennomføre transaksjonene.

Høyesteretts avgjørelse i Rt. 2004 s. 499 gir lite veiledning utover at kundens handlemåte må representere et markert avvik fra vanlig forsvarlig handlemåte, og kundens opptreden må være sterkt klanderverdig slik at vedkommende er vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet. Aktsomhetsvurderingen må for det første knyttes til måten kontakten finner sted på, og for det andre til innholdet i selve meldingen. Sistnevnte har igjen flere sider, herunder utformingen av meldingen, hvordan språket er og hva selve henvendelsen gjelder.

[101] Eksempelvis BKN-2009-6.

[102] Eksempelvis BKN-2007-125.

Måten kontakten finner sted på er gjerne gjennom e-post eller tekstmelding. Dette er kommunikasjonsmåter som finansinstitusjoner selv bruker for å komme i kontakt med sine kunder, og det er derfor ingenting ved selve måten kontakten finner sted på som vil innebære at kunden har grunn til å reagere. Informasjon om hvem som er avsender kan avsløre om det er tale om en reell henvendelse eller ikke. I mange tilfeller er imidlertid avsenderadressen tilnærmet lik, eller manipulert til være identisk med, den banken selv vanligvis benytter. Dette medfører at vurderingen i de fleste tilfeller vil måtte bero på innholdet i meldingen. Flere elementer ved innholdet i meldingen kan avsløre at det ikke er tale om en reell henvendelse. Det første er den grafiske utformingen og selve oppsettet. Amatørmessig utformede e-poster vil gi kunden grunn til å reagere på om henvendelsen er reell. Dernest kan språket være avslørende, hvor et dårlig språk vil være et tegn på at det ikke er kundens faktiske bank som tar kontakt. Denne vurderingen vil påvirkes av kundens personlige forutsetninger, slik som språkkunnskap, jf. over i punkt 3.4. Skrivefeil er ikke i seg selv påfallende, det er det samlede inntrykket som må være avgjørende. Også innholdet i selve henvendelsen er sentralt. Kjernen er at kunden settes under et falskt tidspress for å følge en digital lenke som sender kunden til narresiden. Eksempelvis kan kunden bes om å følge en lenke til «nettbanken» for å oppdatere utløpt informasjon.

I forlengelse av dette er kundens handlingsalternativer sentralt. På den ene side kan kunden avstå fra å trykke på slike lenker i sin helhet. Dette innebærer en risiko for å gå glipp av viktig informasjon som blir tilsendt kunden, slik at dette ikke kan anses som et reelt alternativ. På den andre side kan kunden forsøke å ta kontakt med aktøren for å bekrefte meldingens autentisitet. Det er imidlertid ikke nødvendigvis enkelt for kunden å vite hvor man skal henvende seg. Et praktisk eksempel er at Oslo kommune i februar 2021 sendte e-poster til eldre innbyggere og ba dem om å registrere seg med BankID dersom de ønsket vaksine mot covid-19.[103] Dersom noen av disse innbyggerne hadde fått en fiktiv e-post fra en svindler, men tok kontakt med Oslo kommune for å verifisere henvendelsen, ville vedkommende fått beskjed om at e-posten var reell.

Det foregår omfattende informasjonskampanjer rettet mot forbrukere,[104] og Høyesterett har uttrykkelig slått fast at kunden «må ta hensyn til» at det finnes profesjonelle svindelmetoder.[105] Prinsippet som Høyesterett uttrykker er relevant også ved phishing. Det vil si at når slik svindel er et kjent fenomen, vil det etter omstendighetene kunne stilles strengere krav til kundens aktsomhet. Det kan imidlertid være vanskelig å skille de reelle henvendelse fra

[103] Nissen (2021).

[104] Forbrukertilsynet (2017).

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

svindelforsøkene, all den tid både offentlige og private aktører, herunder banker og diverse abonnementstjenester, faktisk sender slike meldinger til forbrukere.[106] Mens forbrukere på den ene side gjennom informasjonskampanjer frarådes fra å trykke på digitale lenker og oppgi BankID-passord, driver seriøse aktører på den andre side nettopp med å sende slike henvendelser til kunder og innbyggere. Så lenge dette er tilfellet, kan det faktum at kunden har blitt lurt til å falle for en slik henvendelse ikke alene være tilstrekkelig for å konstatere grov uaktsomhet.

Det er i dag ingen publiserte rettsavgjørelser som omhandler spørsmålet om skyld ved phishing ved ikke godkjente betalingstransaksjoner. Finansklagenemnda har imidlertid hatt en rekke av disse sakene til behandling, og i motsetning til betraktningene over har nemnda hovedsakelig ansett det som grovt uaktsomt å falle for phishing.

Finansklagenemnda konkluderte i FinKN-2021-107 med at kunden hadde opptrådt grovt uaktsomt da vedkommende fulgte en lenke som ble tilsendt på e-post og som tilsynelatende kom fra Netflix. Kundens betalingskort var én måned fra å utløpe, og kunden forsto e-posten slik at hun måtte oppdatere betalingsinformasjon på nettsiden. Nemnda la vekt på at kunden burde oppdaget at avsenderadressen og nettadressen på narresiden ikke tilhørte Netflix, og at språket i e-posten var dårlig. Kunden ringte det oppgitte telefonnummeret for å verifisere henvendelsen, og kom til automatisk svarer hos reelle Netflix. Kunden fattet dermed ikke mistanke om svindel, sml. med eksemplet med Oslo kommune over. Nemnda legger midlertid ikke noe vekt på at kunden forsøkte å verifisere e-posten. Ved vurderingen av om pliktbruddet var grovt uttalte nemnda at med «den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle, mener nemnda det må regnes som grovt uaktsomt å la seg svindle på denne måten». Avgjørelsen viser hvordan et samspill av flere momenter som er egnet til å avsløre phishing kan medføre at kunden holdes ansvarlig for et grovt uaktsomt pliktbrudd, til tross for åpenbare momenter som taler i kundens favør.

I FinKN-2020-455 fikk kunden en e-post, som tilsynelatende var fra kundens bank, hvor det fremgikk at kundens bankkort var sperret. For å oppheve «sperringen» måtte kunden følge en lenke. Kunden trodde «sperringen» kunne ha sammenheng med at han hadde vært på handelsmesser. Flertallet mente avsenderadressen ikke var troverdig, og at det heller ikke ga mening at sperringen kunne oppheves ved å følge en lenke, uten at kunden forsikret seg om at det var foretatt uautoriserte transaksjoner først. Nemnda uttalte at «[n]år budskapet i en e-post om mottakerens bankkonto ikke har en god forklaring og et fornuftig innhold, må mottakeren kontrollere hvem som er avsender før han følger en lenke og gir fra seg kort- og sikkerhetsopplysninger». I kombinasjon med at slik svindel etter flertallets oppfatning er

[106] Kjørven (2020) s. 93.

«allment kjent», ble dette ansett som grovt uaktsomt. Mindretallet påpekte imidlertid at e-posten var profesjonelt utformet og at avsenderadressen var troverdig. Dette i kombinasjon med at kunden hadde vært på handelsmesser, medførte etter mindretallets syn at kunden hadde mindre grunn til å reagere på e-posten, og mente at dette ikke kunne utgjøre grov uaktsomhet.

Sakene viser at Finansklagenemnda i mindre grad er villige til å legge vekt på konkrete forhold ved den enkelte henvendelsen som kan medføre at kunden ikke har grunn til å reagere, og vektlegger selve budskapet i henvendelsen i stor grad. Dette var også tilfellet i FinKN-2019-681, hvor kunden ifølge flertallet handlet grovt uaktsomt når han fulgte en lenke hvor det fremgikk at vedkommende hadde bestilt ekstra lagringsplass til sin mobiltelefon, en tjeneste kunden hadde brukt før. I denne saken er mindretallets bemerkninger av særlig interesse, ettersom de uttrykkelig fremhevet at til tross for generelle advarsler så fremsto slik svindel som et utbredt og omfattende problem som var «vanskelig å komme til livs». Med henvisning til rapporter fra Økokrim fremhevet mindretallet at det ligger i dagen at begrunnelsen er manglende kunnskap hos næringsdrivende og særlig privatpersoner. Dette er et sentralt poeng som må ha stor betydning for aktsomhetsvurderingen ved denne typen svindel. Det er en grense for hvor mange slike saker Finansklagenemnda kan behandle samtidig som de opprettholder det standpunkt at kunden i det store flertallet av sakene har handlet grovt uaktsomt. Mindretallet vektla i denne saken at kundens oppmerksomhet naturlig vil senkes når avsender tilsynelatende er kjent, og henvendelsen for øvrig fremsto autentisk.[107]

Nemndas begrunnelse i tilsvarende saker bygger hovedsakelig på en kombinasjon av at de anser det som allment kjent at slik svindel skjer og at det foreligger elementer ved den enkelte melding som er egnet til å skape tvil om den er reell.[108] I de tilfellene nemnda har konkludert at det ikke foreligger grov uaktsomhet, har dette vært begrunnet i sakenes spesielle omstendigheter. Eksempelvis ble kunden i FinKN-2018-311 gjennom e-post angivelig kontaktet av kortutsteder, hvor kunden ble bedt om å oppgi opplysninger for å fjerne sperren fra et bankkort. Kunden ble deretter utsatt for svindel. I dette tilfellet hadde imidlertid kunden i forkant selv forsøkt å sperre kortet, men fikk ikke kontakt med betalingstjenesteyteren. Nemnda mente at dette utgjorde såpass spesielle omstendigheter at kunden ikke kunne anses å ha handlet grovt uaktsomt.[109]

Disse sakene utgjør imidlertid unntaket til Finansklagenemndas nokså strenge praksis hvor det som hovedregel foreligger grov uaktsomhet dersom kunden har fulgt en digital lenke for så å oppgi nødvendig informasjon på en narreside. Sammenlignet med praksis fra andre EU-land, virker praksis i Norge å følge en strengere aktsomhetsnorm i tilsvarende saker.

---

[107] Tilsvarende i FinKN-2019-683.

[108] Se eksempelvis FinKN-2019-565, FinKN-2019-40, FinKN-2018-530 og FinKN-2017-649.

[109] Tilsvarende i FinKN-2019-336 og FinKN-2019-338.

I Danmark har det Finansielle Ankenævn konkludert med at kunden ikke har handlet grovt uaktsomt i tilsvarende saker. I eksempelvis sak 290/2018 hadde kunden fått en e-post hvor det fremgikk at vedkommendes konto ville bli belastet hvis ikke en betalingstransaksjon ble avbrutt. Kunden trykket på lenken og oppga nødvendig informasjon som muliggjorde at svindlere belastet kundens konto. Ankenævnet konkluderte med at kunden ikke hadde handlet grovt uaktsomt ettersom henvendelsen fremstod som troverdig.

Heller ikke i Storbritannia konkluderer The Financial Ombudsman med grov uaktsomhet i lignende saker. I sak DRN-4082710 hadde kunden fått en e-post hvor det fremgikk at kundens konto hadde blitt sperret. Kunden hadde nylig gjennomført en betalingstransaksjon, og trodde sperringen hadde sammenheng med dette. Kunden ble svindlet etter at han oppga sikkerhetsinformasjon på en narreside. The Financial Ombudsman la vekt på at e-posten fremsto som troverdig og at kunden av den grunn ikke hadde grunn til å reagere. Ettersom e-posten og nettsiden kunden ble dirigert til var overbevisende, kunne ikke kunden anses å ha handlet grovt uaktsomt. Heller ikke i sak DRN-4139348 kom The Financial Ombudsman til at det var tale om grov uaktsomhet. Kunden hadde fått en e-post som ba han verifisere e-posten sin ved opprettelsen av en betalingskonto, og var identisk med e-posten som kunden tidligere hadde fått fra betalingstjenesteyteren. Ved å følge lenken i e-posten ga kunden svindleren tilgang til kontoen. Utgangspunktet for vurderingen var om kundens handlinger «fell so far below the standard of a reasonable person», slik at det utgjorde grov uaktsomhet. Det slås uttrykkelig fast at det å dele sikkerhetsinformasjon ved slik svindel ikke alene kan utgjøre grov uaktsomhet. Ettersom både e-posten og narresiden fremsto troverdig, kunne ikke kundens handlinger anses å utgjøre et markert avvik fra vanlig forsvarlig handlemåte. Det er avsagt en rekke avgjørelser hvor The Financial Ombudsman har kommet til samme resultat.[110] Praksisen viser at de ikke anser det som grovt uaktsomt å falle for velgjennomført og profesjonell phishing.

Gjennomgangen viser at foreliggende praksis i Norge hittil har gått nokså langt i å definere aktsomhetsnormen etter hvordan en idealkunde ville handlet, og dermed forlates i stor grad utgangspunktet i Rt. 2004 s. 499 om at det er de kvalifisert klanderverdige tilfellene faller under betegnelsen «grovt uaktsomme» pliktbrudd. Finansklagenemnda anser det tilstrekkelig for grov uaktsomhet at kunden har latt seg lure til å trykke på en lenke og oppgi innloggingsinformasjon, uten nærmere drøftelse av kundens forutsetninger for å avdekke om det er tale om reell henvendelse eller konkrete omstendigheter i saken. Kun ved helt spesielle omstendigheter har nemnda unntaksvis konkludert med at kunden ikke har handlet grovt uaktsomt. I lys av hvordan terskelen for grov uaktsomhet er tolket og anvendt av Høyesterett, kan nemndas praksis hva

[110] Se eksempelvis DRN-2174713, DRN-5688949 og DRN-4773354.

angår phishing etter min oppfatning ikke anses som uttrykk for en riktig anvendelse av aktsomhetsterskelen. Særlig i tilfeller der henvendelsen fremstår som ekte har det i liten grad funnet sted en vurdering av kundens bebreidelse. At kunden ikke oppfatter en slik henvendelse som et svindelforsøk er desto mer unnskyldelig ettersom offentlige og private aktører sender lignende henvendelser til sine kunder. Nemnda tok nettopp opp denne problematikken i FinKN-2018-46, men valgte å avvise saken fra nærmere behandling. Nemnda påpeker at de har erfart at BankID som innloggingsverktøy brukes av flere aktører enn forutsatt i tidligere saker, som etter nemndas syn gjør det mindre påfallende og mistenkelig å bli anmodet om å logge inn med BankID. Videre påpekes det at dette kan skape inntrykk av at det er trygt på følge lenker for så å taste innloggingsinformasjon, som igjen har innvirkning på skyldvurderingen. Tilsvarende synspunkter er fremhevet av Finanstilsynet, hvor kombinasjonen av den utstrakte bruken av BankID og variasjoner i innloggingskontekst medfører en «slitasje» på BankID og kundens kritiske sans.[111] Nemndas uttalelser har imidlertid hatt lite å si for etterfølgende praksis.

3.6 Sammenfatning

Vurderingstemaet for grov uaktsomhet er hvorvidt det foreligger et markert avvik fra vanlig forsvarlig handlemåte, slik at det dreier seg om en opptreden som er sterkt klanderverdig hvor kunden er vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet. Dette utgangspunktet følger også av fortalen til PSD 2 punkt 72. Målestokken er den alminnelige bankkunde, og det avgjørende er en samlet bedømmelse av den konkrete saken.

Ved tredjepersons misbruk av betalingskort og tilhørende kode, tyder etterfølgende praksis på at terskelen for grov uaktsomhet har blitt praktisert på linje med Høyesteretts forutsetninger i Rt. 2004. s. 499. Denne praksisen må anses å være retningsgivende også for tilfeller av ikke godkjente betalingstransaksjoner etter finansavtaleloven (2020). Enkeltavgjørelser er avvikende, og tyder på at nemnda har lagt terskelen for grov uaktsomme pliktbrudd høyere enn det tilsynelatende er grunnlag for. Enkeltstående avgjørelser fra Finansklagenemnda har imidlertid svært begrenset rettskildeverdi.

Praksis i tilknytning phishing antyder at Finansklagenemnda har etablert en linje hvor terskelen for grov uaktsomhet er satt såpass lavt at kunden nærmest holdes objektivt ansvarlig for en egenandel på 12 000 kroner dersom kunden faller for slik svindel. Dette kan neppe anses å være i overenstemmelse med den terskelen for grov uaktsomhet som Høyesterett har trukket opp. Etter min oppfatning måles kunden etter hvordan en idealkunde hadde handlet, noe Høyesterett nettopp avfeier skal være målestokken for grov uaktsomhet. Omfanget av praksisen viser at den alminnelige bankkunde i mange tilfeller lar seg lure av disse målrettede og profesjonelle

[111] Finanstilsynet (2021) s. 25.

svindelforsøkene. Sett i sammenheng med at nemnda selv innrømmer at både offentlige og private aktører sender e-poster der privatpersoner bes om å oppgi BankID-passord, virker det svært strengt å holde kunden ansvarlig for grovt uaktsomme pliktbrudd når meldingen ellers ved ganske stor presisjon illuderer en reell henvendelse. Inntil det foreligger en autorativ avgjørelse fra de alminnelige domstolene som tilsier noe annet, kan ikke denne nemdspraksisen anses å være retningsgivende for forståelsen av terskelen for grov uaktsomhet ved phishing.

4 Terskelen for forsettlige pliktbrudd

4.1 Innledning

Kunden svarer for hele det økonomiske tapet ved ikke godkjente betalingstransaksjoner dersom kunden «forsettlig har misligholdt sine plikter slik at kunden måtte forstå at misligholdet kunne innebære en nærliggende fare for at betalingsinstrumentet kunne bli misbrukt», jf. § 4-30 fjerde ledd. Med «sine plikter» menes kundens forpliktelser etter § 4-23 og § 4-24. Spørsmålet her er hva som nærmere ligger i finansavtalelovens forsettkrav, som vil behandles nærmere i punkt 4.2. I punkt 4.3 vil betydningen av villfarelse nærmere belyses, før det i punkt 4.4 vil redegjøres for utvalgte typetilfeller av misbruk av betalingsinstrumenter hvor forsett kan være aktuelt.

Innledningsvis påpekes det at ved vedtakelsen av ny finansavtalelov så ble mindretallets forslag i Innst. 104 L (2020-2021) på enkelte punkter vedtatt av Stortinget.[112] Det sentrale her gjelder forsettbegrepet, hvor mindretallets merknader i innstillingen avviker fra de i proposisjonen og følgelig gir uttrykk for hva som vil være gjeldende rett ved lovens ikrafttredelse.

4.2 Om forsettbegrepet i finansavtaleloven

4.2.1 Historisk kontekst

For å forstå forsettkravet i finansavtaleloven (2020), er det hensiktsmessig å se på begrepets historiske utvikling. Etter finansavtaleloven (1999), slik den lød da den ble vedtatt, svarte kunden for hele tapet dersom vedkommende «forsettlig har muliggjort bruken av kortet», jf. daværende § 35. Tilsvarende gjaldt for misbruk av konto, jf. daværende § 34. Ansvaret var altså betinget av at kunden bevisst utstyrte en tredjeperson med *muligheten* til å bruke betalingsinstrumentet, og forarbeidene eksemplifiserte dette med at forsettkravet var oppfylt dersom kunden lånte bort betalingsinstrumentet for hjelp til å heve 500 kroner.[113]

Dersom en tredjeperson imidlertid urettmessig tilegnet seg betalingsinstrument og kode, kunne situasjonen være en annen. I BKN-2005-163 betalte kunden for en drosjetur mens sjåføren så på, og nemnda uttalte at forsettkravet innebar at

> «kortholder ved sin opptreden i drosjen må ha holdt det for sikkert eller overveiende sannsynlig at kortet ville bli misbrukt. Det er således ikke tilstrekkelig for å statuere ansvar etter forsettbestemmelsen i fil. § 35 (4) at selve tapet av kort og kode ligger innenfor kortholders forsett».

Dette antyder at det gikk et skille mellom tilfellene der kunden selv utstyrer en tredjeperson med muligheten til å misbruke kortet, og tilfeller der en tredjeperson urettmessig tilegner seg

[112] Lovvedtak 24 (2020-2021).

[113] NOU 1994:19 s. 74.

dette.[114] I forarbeidene til finansavtaleloven (1999) følger det uttrykkelig at «forsettet – i samsvar med vanlige skyldprinsipper – må henspeile seg på både selve handlingene og konsekvensen av handlingen».[115] Uttalelsene uttrykker at også *følgen* av pliktbruddet må være omfattet av kundes forsett, slik også Bankklagenemnda la til grunn over. Videre uttales imidlertid at

> «tapet normalt må anses voldt forsettlig dersom *kunden har overlatt* brukerlegitimasjonen til et familiemedlem som i betydelig grad har belastet kontoen eller belastet den ut over den grensen kontohaveren har fastsatt. I slike tilfeller kan for øvrig fullmaktsbetraktninger føre til samme resultat. I tilfelle hvor en *tredjemann har tilegnet seg* nødvendig brukerlegitimasjon og misbrukt kontoen, vil forholdet sjelden være at kunden bevisst har utvist en så høy grad av uforsiktighet ved oppbevaringen av den nødvendige brukerlegitimasjonen at tapet kan sies å være voldt ved forsettlig handlemåte fra kundens side.»[116] (min utheving)

Også her gikk det altså et skille mellom tilfellene der kunden utstyrer en tredjeperson med muligheten til å bruke betalingsinstrument, og tilfellene der en tredjeperson urettmessig tilegner seg dette. Det trekkes en parallell til fullmaktsoverskridelse, der en godtroende tredjeperson etter omstendighetene kan holde fullmaktsgiver ansvarlig for fullmakthavers disposisjon.[117] Med andre ord kunne man ut fra disse uttalelsene trekke et skille mellom tilfellene der tredjeperson utleder sin rett til å bruke betalingsinstrumentet fra rettmessig innehaver eller ikke.

Dersom en tredjeperson urettmessig tilegner seg betalingsinstrumentet og koden, ble vurderingen om kunden «bevisst har utvist en så høy grad av uforsiktighet ved oppbevaringen av den nødvendige brukerlegitimasjonen».[118] Dette er en vurdering av i hvilken grad kunden bevisst har handlet klanderverdig. Det kan her trekkes en parallell til hvordan forsettkravet er forstått i erstatningsretten, hvor forsett er betinget av at kunden er klar over handlingen og handlingens skadepotensiale, se nærmere om dette under punkt 4.2.2.[119]

---

[114] I motsetning til oppfatningen etter lov av 21. juni 1985 om kredittkjøp mm., som er forløperen til finansavtaleloven (1999), hvor Bankklagenemnda i BKN-1995-47 uttalte at «[e]tter kredittkjøpsloven § 13 må forsettet bare omfatte selve tapet av kortet».

[115] NOU 2008:21 s. 97.

[116] NOU 2008:21 s. 98.

[117] Giertsen (2014) s. 293 flg.

[118] NOU 2008:21 s. 98.

[119] Nygaard (2007) s. 166.

4.2.2 Tolkning av forsettbegrepet

Ansvarsbegrensningene i finansavtaleloven (2020) § 4-30 bortfaller dersom kunden «forsettlig» misligholder sine plikter på en slik måte at kunden «måtte forstå» at det var en «nærliggende fare» for misbruk. Dette reiser tre spørsmål, nemlig hva som ligger i «forsettlig» mislighold, «måtte forstå» og «nærliggende fare».

Det første spørsmålet er hva som ligger i utrykket «forsettlig» mislighold. Forsettbegrepet er utviklet innenfor strafferetten,[120] og knytter seg til gjerningsmannens bevissthetsforestillinger på handlingstidspunktet.[121] Skyldkravet har innenfor strafferetten en restriktiv funksjon, hvor det setter grenser for når og hvor strengt man kan – og bør – straffe.[122] I privatretten er funksjonen av mer dynamisk karakter, hvor det utgjør en positiv begrunnelse for plassering av ansvar og risiko. Det er tale om en gradering av ansvaret, hvor ansvaret avpasses etter skyldgraden.[123]

Innenfor kontraktsretten er det bred enighet om at de forsettlige avtalebruddene er forbeholdt tilfellene der kontraktsparten *bevisst* tilsidesetter medkontrahentens interesser og handler i strid med kontraktens normer.[124] Utgangspunktet er på denne bakgrunn at det «forsettlige» misligholdet innebærer at kunden bevisst har handlet i strid med sine lovpålagte forpliktelser.

I teorien har det vært omfattende diskusjoner om det kontraktsrettslige forsettbegrepet omfatter følgene av pliktbruddet, eller om bevissthet om overtredelse av kontraktsforpliktelsene er tilstrekkelig.[125] Lovgiver har for finansavtalelovens vedkommende løst dette ved at det etter § 4-30 fjerde ledd i tillegg til det «forsettlige» misligholdet kreves at kunden «måtte forstå» at misligholdet kunne innebære en «nærliggende fare» for misbruk av betalingsinstrumentet.

Dette bringer oss over til *det andre* spørsmålet, nemlig hva som ligger i vilkåret om at kunden «måtte forstå» at det var fare for misbruk. Ordlyden virker å ta sikte på kundens forståelse av farenivået på handlingstidspunktet, og avgrenser mot tilfellet der kunden *burde* ha forstått at det forelå en nærliggende fare for misbruk. Det oppstilles heller ikke et krav om positiv

---

[120] Hagstrøm (2011) s. 479.

[121] Andenæs (2016) s. 234.

[122] Krüger (1968) s. 45.

[123] Flere har tatt til orde for at forsettsterminologien i liten grad er egnet som et avgjørende kriterium for plasseringen av et slikt ansvar. Dels kan dette begrunnes i skyldkravets ulike funksjon i strafferetten og i privatretten, se Krüger (1968) s. 60 og Hagstrøm (2011) s. 479. Dels kan det begrunnes med at bevisste handlinger ikke nødvendigvis innebærer en økt grad av bebreidelse som kan begrunne et mer omfattende ansvar, se Kaasen (2005) s. 253.

[124] Se eksempelvis Krüger (1989) s. 784 flg., Kaasen (2005) s. 253, Bruserud (2010) s. 128 og Hagstrøm (2011) s. 70 og 479.

[125] Hagstrøm (2011) s. 479.

kunnskap om faren. Forarbeidene fremhever at forsettkravet ikke er oppfylt dersom kunden har bedt om bistand for å betale regninger, ettersom kunnskap om «den personlige sikkerhetsinformasjon ikke alene er tilstrekkelig til å utføre misbruk, kan det at uvedkommende kjenner slik informasjon, heller ikke alene være tilstrekkelig for å si at vedkommende måtte forstå at det forelå en nærliggende fare for misbruk».[126] Det kreves noe utover dette for at kunden «måtte forstå» at det misbruk er en fare.

En rekke bestemmelser innenfor kontraktsretten benytter tilsvarende formuleringer, slik som reglene om realkreditors opplysningsplikt i avhendingsloven § 3-7[127] og kjøpsloven § 17 annet ledd bokstav b.[128] Høyesterett slo fast i Rt. 2002 s. 1110 på s. 1120 at uttrykket innebærer at det for kontraktsparten ikke kunne være «noen rimelig unnskyldning for å være uvitende om forholdet».[129] Den rådende oppfatning i teorien er på bakgrunn av dette at det stilles krav til at den misligholdende kontraktspart må ha opptrådt grovt uaktsomt med hensyn til konsekvensene av kontraktsbruddet.[130]

Forarbeidene til finansavtaleloven (2020) slår imidlertid fast at forsettkravet vil samsvare med de tilsvarende reglene i Sverige og Danmark, som videre 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».[131] Forarbeidene antyder med dette at det må foreligge sannsynlighetsforsett med hensyn til følgen av kundens pliktbrudd. Forarbeidene legger dermed til grunn, i motsetning til oppfatningen i kontraktsrettslitteraturen, at det ikke er tale om et krav til uaktsomhet med hensyn til konsekvensene av pliktbruddet.

I erstatningsretten er behovet for å avgrense mot de grovere skyldformene underordnet, da det for etableringen av erstatningsansvaret er uten betydning hvilken grad av skyld skadevolder har utvist.[132] Forsett foreligger når skadevolderen har villet følgene av handlingen eller er bevisst at det er sannsynlighetsovervekt for at skaden vil inntre.[133] Dette samsvarer imidlertid ikke med slik kriteriet «måtte forstå» er tolket i erstatningsretten. I Rt. 1978 s. 321, som gjaldt et forsikringsselskaps erstatningsansvar etter bilansvarsloven § 7,[134] uttalte Høyesterett at «[e]tter

[126] Innst. 104 L (2020-2021) s. 21-22.
[127] Lov av 3. juli 1992 nr. 93 om avhending av fast eigedom.
[128] Lov av 13. mai 1988 nr. 27 om kjøp.
[129] Tilsvarende i Rt. 2002 s. 696 på s. 702.
[130] Slik Hagstrøm (2011) s. 163 og Bruserud (2011) s. 58-59.
[131] Innst. 104 L (2020-2021) s. 22.
[132] Kjelland (2019) s. 96.
[133] Wilhelmsen og Hagland (2017) s. 140.
[134] Lov av 3. februar 1961 om ansvar for skade som motorvogner gjer.

vanlig språkbruk ligger det i «måtte forstå» eller «måtte vita» at man har for seg en situasjon som ut fra en normal bedømmelse gjør en mulig uvitenhet uforståelig.» Dette samsvarer med forståelsen av kriteriet «måtte forstå» slik det er tolket i kontraktsretten.

I denne sammenheng har Hagstrøm argumentert for at et krav om sannsynlighetsforsett med hensyn til følgen av pliktbruddet er helt upraktikabelt, ettersom den misligholdende part lett vil frifinnes for å ikke ha holdt følgende som sikre eller overveiende sannsynlige.[135] Det er nettopp av disse grunner at lovgiver i bestemmelser som bygger på forsett innenfor kontraktsretten har innført krav om at kontraktsparten «var eller måtte være kjent», og tilsvarende formuleringer.

Selv om uttalelser i forarbeidene til finansavtaloven (2020), samt tidligere forarbeider og nemndspraksis,[136] kan understøtte et krav om sannsynlighetsforsett, virker dette å stride med ordlyden i § 4-30. Det er altså uklart om det er tale om et krav om sannsynlighetsforsett med hensyn til følgen eller om det siktes til forståelsen av «måtte forstå» slik dette er tolket innenfor erstatningsretten og kontraktsretten.

Forarbeidene forutsetter uten nærmere redegjørelse at forsettkravet vil praktiseres likt som i Sverige og Danmark. I den svenske betalingstjenesteloven benyttes ikke skyldformen forsett.[137] Kunden er etter kapittel 5 a § 3 ansvarlig for 12 000 kroner ved grov uaktsomhet, men må bære hele det økonomiske tapet dersom vedkommende har «handlat särskilt klandervärt». Ordlyden knytter altså ikke ansvar til et bevisst pliktbrudd, men til graden av klanderverdighet ved pliktbruddet.[138] En slik forståelse av forsettkravet kan verken forenes med ordlyden i finansavtaleloven (2020) § 4-30 eller uttalelsene i forarbeidene for øvrig. Dersom henvisningen til svensk rett forstås slik at det kreves en grad av bebreidelse med hensyn til følgen av pliktbruddet, vil dette samsvare med tolkningen av kriteriet «måtte forstå» i norsk kontraktsrett og erstatningsrett. Samtidig utelukker dette sannsynlighetsforsett med hensyn til følgen av pliktbruddet.

I Danmark er kunden som utgangspunkt ansvarlig for hele tapet ved forsettlige pliktbrudd, jf. den danske betalingsloven § 100 annet ledd.[139] Dette presiseres imidlertid i femte ledd, som omhandler kundens ansvar for å verne om personlig sikkerhetsinformasjon. Kunden hefter etter denne bestemmelsen for hele det økonomiske tapet dersom kunden forsettlig har opplyst personlig sikkerhetsinformasjon til en tredjeperson og «indså eller burde have indset, at der var

[135] Hagstrøm (2011) s. 479-480.
[136] Jf. punkt 4.2.1.
[137] Lag (2010:751) om betaltjänster.
[138] Kjørven (2020) s. 96.
[139] Lov nr. 652 af 8. juni 2017 om betalinger.

risiko for misbrug». Ansvarsbegrensningene bortfaller altså dersom det foreligger et bevisst pliktbrudd, *og* det i det minste forelå uaktsomhet med hensyn til tapet. Dette kan ikke umiddelbart forenes med uttalelsene i forarbeidene til finansavtaleloven (2020). Dersom henvisningen imidlertid forstås slik at det kreves bebreidelse med hensyn til følgen av pliktbruddet, vil dette som med svensk rett stemme godt med slik kriteriet «måtte forstå» er tolket i norsk kontraktsrett og erstatningsrett.

Henvisningen til svensk og dansk rett impliserer at det stilles et krav om bebreidelse med hensyn til konsekvensen av pliktbruddet, samtidig som det utelukker et krav om sannsynlighetsforsett. På bakgrunn av en slik uklarhet i forarbeidene er det mest nærliggende å ta utgangspunkt i en naturlig språklig forståelse av ordlyden, hvor utgangspunktet må være kundens oppfatning av farenivået i den konkrete situasjonen. Slik uttrykket er forstått i erstatningsretten og i kontraktsretten, er det avgjørende om det ikke kunne være «noen rimelig unnskyldning for å være uvitende» om at misbruk ville skje. Dersom det etter en normal bedømmelse av situasjonen fremstår som uforståelig at kunden var uvitende om faren for misbruk, vil forholdet måtte bedømmes slik at kunden «måtte forstå» dette. Dette vil ligge nærmere opp til forståelsen av det tilsvarende kravet i Sverige og Danmark enn et krav om sannsynlighetsforsett.

For det tredje må det avklares hva som ligger i uttrykket «nærliggende fare» for at misbruk kan oppstå. Ordlyden virker å ta sikte på at det i forkant av pliktbruddet objektivt sett må foreligge en reell mulighet at misbruk av betalingsinstrumentet kunne skje som følge av kundens handlinger. At denne faren må være «nærliggende» forstås slik at det avgrenses mot perifere faresituasjoner. Ved vurderingen vil sannsynligheten for at misbruk kan skje være sentralt.

I denne sammenheng er det avgjørende å avklare om det siktes den generelle eller den konkrete faren for at misbruk som kan oppstå. Det kan hevdes at det alltid vil være en fare for at betalingsinstrumentet blir misbrukt dersom man deler sikkerhetsinformasjon. Av forarbeidene følger det imidlertid at det å dele kode eller passord med en tredjeperson ikke nødvendigvis vil utgjøre et forsettlig pliktbrudd.[140] Forarbeidene impliserer altså at det må foreligge andre omstendigheter enn det faktum at kunden har delt sikkerhetsinformasjon med en tredjeperson. Hvorvidt slike omstendigheter foreligger, må nettopp vurderes ut fra de konkrete forholdene i saken. Dette kan eksempelvis være hvordan kunden oppbevarer betalingsinstrumentet, eller om det foreligger andre omstendigheter som gir grunn til å reagere på hjelperens hensikt. På denne bakgrunn forstås det at bestemmelsen sikter til den konkrete faren i det individuelle tilfellet.

Dersom det objektivt sett foreligger en reell mulighet for misbruk av kundens betalingsinstrument i den konkrete situasjonen, vil det i finansavtalelovens forstand måtte anses

[140] Innst. 104 L (2020-2021) s. 21.

som at det foreligger en «nærliggende fare» for misbruk. Dersom kunden i tillegg har handlet bevisst, og slik at han «måtte forstå» at handlingene ville medføre en slik fare, er alle vilkårene for at ansvarsbegrensningene bortfaller til stede.

4.3 Betydningen av uvitenhet om rettslige og faktiske omstendigheter

Det kan reises spørsmål om skyldvurderingen påvirkes av at kunden er i rettslig eller faktisk villfarelse. Her vil det først redegjøres for betydningen av rettsvillfarene, før faktisk villfarelse vil bli behandlet. Problemstillingen er særlig aktuell i de tilfellene betalingstjenesteyteren gjør gjeldende at kunden er skyldig i et forsettlig pliktbrudd, men kunden innvender at vedkommende har feilbedømt situasjonen eller var uvitende om sine forpliktelser.[141]

Hva angår *rettsvillfarelse*, har det i kontraktsrettslig teori i lang tid vært hevdet at «rettsvillfarelse skader alltid».[142] På denne bakgrunn sies det at det for kontraktsrettslige forpliktelser gjelder et objektivt erstatningsansvar ved rettsvillfarelse.[143] Det er altså tale om et selvstendig ansvarsgrunnlag ved mislighold som beror på rettsvillfarelse. Det må imidlertid understrekes at også dette ansvaret er gradert, slik at det lett kan tenkes at misligholderen pålegges et ansvar uten at det samtidig er tale om forsett, til tross for at det dreier seg om bevisste handlinger.[144] Dette er et sentralt poeng i tilknytning finansavtalelovens ansvarsregler – det ligger ingen automatikk i at kunden er ansvarlig for et forsettlig pliktbrudd alene på det grunnlag at kunden var uvitende om sine rettslige forpliktelser. Skyldgraden må vurderes konkret.

Av proposisjonen til finansavtaleloven følger det at det for vurderingen av om kunden har utvist forsett, er uten betydning at kunden ikke var kjent med sine forpliktelser. Det presiseres imidlertid at villfarelse om forpliktelsene som følger av utstedelsesavtalen om håndteringen av sikkerhetsopplysninger kan anses som unnskyldelig etter «alminnelige regler».[145] Selv om uttalelsene knytter seg til forsettkravet før ordlydsendringen, er disse av slik generell karakter at de også er av relevans for forståelsen av forsettkravet etter ordlydsendringen.

I motsetning til i kontraktsretten generelt, så er ikke spørsmålet etter finansavtaleloven (2020) § 4-30 om kunden skal holdes erstatningsansvarlig for et mislighold, men om kunden kan påberope seg de lovfestede ansvarsbegrensningene. Ansvarsfordelingen styres av skyldvurderingen etter § 4-30, hvor en eventuell villfarelse kan ha innvirkning på denne vurderingen, men kan ikke i seg selv begrunne et ansvar utover lovens ansvarsbegrensninger.

---

[141] Eksempelvis ved «vishing», se nærmere under punkt 4.4.

[142] Arnholm (1973) s. 293 og Augdahl 1978 s. 227.

[143] Hagstrøm (2011) s. 527.

[144] Krüger (1968) s 79.

[145] Prop. 92 LS (2019-2020) s. 186.

Det er altså ikke slik at rettsvillfarelse kan fungere som et selvstendig ansvarsgrunnlag for å pålegge kunden et erstatningsansvar utover lovens ansvarsbegrensninger. Det følger verken av gjeldende eller ny finansavtalelov at forbrukeren pålegges et objektivt ansvar for forståelsen av og innholdet i utstedelsesavtalen.

Risikobetraktninger tilsier at det klare utgangspunktet må være at kontraktsparten selv bærer risikoen for sin egen forståelse av kontraktsforpliktelsene. Dette gjelder med styrke der begge partene har vært med på å utforme avtalen. Andre hensyn enn i kontraktsretten generelt gjør seg imidlertid gjeldende i tilfellet der en profesjonell tjenestetilbyder inngår en avtale om finansielle tjenester med en forbruker. Utstedelsesavtalen er i sin helhet utformet og diktert av betalingstjenesteyteren, uten at kunden har vært med på å utforme kontraktens adferdsnormer. Utgangspunktet om at «rettsvillfarelse skader alltid» er ikke like opplagt der den svakere kontraktspart i realiteten underlegges medkontrahentens bestemmelser om kontraktens forpliktelser.[146] Dersom kunden har hatt en uriktig, men likefult forsvarlig, forståelse av kontraktsforpliktelsene, vil reelle hensyn tale for å anse rettsvillfarelsen som ansvarsfri. Falkanger trekker frem at disse tilfellene har nært slektskap til synspunktene som er gjort gjeldende i forbindelse med erstatningsansvar for ugyldige forvaltningsvedtak.[147] Oppfatningen er at en kommune bare holdes erstatningsansvarlig dersom det foreligger klanderverdig rettsvillfarelse, mens staten vil være objektivt ansvarlig. Begrunnelsen for forskjellen er at det er staten, og ikke kommunene, som har utformet reglene. Slik er nettopp forholdet mellom kunden og betalingstjenesteyteren.

I erstatningsretten åpnes det i større grad for at rettsvillfarelse kan frita for ansvar, men også her er det tale om en streng norm.[148] I Rt. 1995 s. 1350 var spørsmålet om en eiendomsmegler og en takstmann kunne holdes erstatningsansvarlige for et salg av en bolig hvor underetasjen ikke var godkjent til beboelse. Retten uttalte at de klart ikke kunne «bebreides for en eventuell rettsvillfarelse på dette punktet» ettersom det var tale om perifere rettsregler. Prinsippet som her uttrykkes, om at en villfarelse som parten ikke kan bebreides for er ansvarsfri, vil med styrke måtte gjelde i forbrukerforhold. Dette uttrykte også Finansklagenemnda i FinKN-2020-707, som gjaldt vishing-svindel:

> «Selv om man skal være forsiktig med å trekke slutninger fra andre rettsområder, mener flertallet at lovgivning og rettspraksis som nevnt kan bidra til å vise at rettslig villfarelse som ikke kan bebreides vedkommende part, kan ha betydning ved vurderingen av om lovfestede eller ulovfestede skyldkrav er oppfylt.

[146] Falkanger (1997) s. 124.

[147] Falkanger (1997) s. 124, note 4.

[148] Hagstrøm og Stenvik (2019) s. 167.

Kunden kunne ikke bebreides for manglende kjennskap til utstedelsesavtalens forbud mot å røpe engangskoder og passord. En slik forståelse, hvor det er kundens *bebreidelse* som er det sentrale, vil stemme godt overens med de overnevnte hensyn og kontraktsrettens system hvor ansvaret graderes ut fra utvist skyld, se punkt 4.2.2. Kunden kan ha handlet bevisst uten at det er tale om en klanderverdig handling. Slik Falkanger uttrykker det, bør ansvarsfrihet være aktuelt der den svakere kontraktspart er i villfarelse om forpliktelser i kontrakten som medkontrahenten har diktert innholdet i.[149] Dette må etter min oppfatning gjelde i enda større grad der en forbruker har inngått en avtale med en profesjonell part. Når kunden har vært aktsomt uvitende om sine forpliktelser, er vitterlig ikke de hensyn som begrunner at ansvarsbegrensningene bortfaller til stede. Terskelen må imidlertid være høy, og det skal ikke mye til før kunden kan bebreides for å ikke kjenne til eller forstå innholdet i kontraktsforpliktelsene.[150]

Situasjonen er samtidig ofte slik at kunden, i tillegg til rettsvillfarelse, også er i *faktisk villfarelse*. Igjen er vishing-tilfellet illustrerende, hvor kunden eksempelvis tror at vedkommende er i kontakt med sin reelle bank for å stoppe utbetalingen av et lån. Spørsmålet blir hvilket utslag dette vil ha på skyldvurderingen.

I motsetning til rettsvillfarelse, har faktisk villfarelse i større grad vært ansett som ansvarsbefriende, der et eventuelt ansvar er betinget av at det er utvist skyld.[151] Dersom en part er aktsomt uvitende om de faktiske forhold, vil den faktiske villfarelse anses som ansvarsfri. Dette kan ha direkte innvirkning på hvorvidt kunden «måtte forstå» at det var en nærliggende fare misbruk, og følgelig på vurderingen av om ansvarsbegrensningene bortfaller, se punkt 4.2.2. Dersom kunden er aktsomt uvitende om de faktiske forhold, og situasjonen slik den oppleves for kunden ikke gir grunn til å tro at misbruk kan skje, må konklusjonen ved skyldvurderingen være at kunden ikke har handlet forsettlig etter § 4-30 fjerde ledd. Dette understreker viktigheten av å vurdere om kunden er i aktsom faktisk villfarelse.

Det kan være vanskelig for kunden å verifisere om henvendelsen er reell. Et nummersøk vil ikke nødvendigvis hjelpe, ettersom svindlere gjennom såkalt «spoofing» kan manipulere nummeret som ringer slik at det fremstår som et annet.[152] Slik kan svindlere eksempelvis skjule seg bak nummeret til kundens bank og forsterke den villfarelse kunden befinner seg i. Svindelen kan avsløres ved at kunden avslutter samtalen og selv tar kontakt med banken, men dette

[149] Falkanger (1997) s. 130.

[150] Se imidlertid punkt 3.4 om betydningen av kundens individuelle forhold.

[151] Lund (1970) s. 59 og Hagstrøm og Stenvik (2019) s. 166.

[152] Næringslivets sikkerhetsråd (2020) s. 57.

handlingsalternativet vil ofte fremstå som fjernt i den konkrete situasjonen, ettersom opplevelsen av tidspress og stress vil gjøre det vanskelig for kunden å orientere seg. Dette gjelder med styrke dersom kontakten for øvrig fremstår troverdig.

Hvis kunden faktisk tror at det er banken som har tatt kontakt, er situasjonen egnet til å vanskeliggjøre kundens oppfatning av hvilke rettslige forpliktelser som påhviler vedkommende. Den faktiske villfarelsen påvirker på denne måten vurderingen av om rettsvillfarelsen kan anses som unnskyldelig. Enda vanskeligere for kunden blir det at en slik situasjon i realiteten kan innebære en endringsavtale. Hvis det faktisk var banken som tok kontakt og av en reell grunn hadde behov for kundens innloggingsinformasjon, må dette avtalerettslig anses som en endring av avtalevilkårene.

Der det ikke er tale om en unnskyldelig *faktisk villfarelse*, vil det neppe kunne være tale om en unnskyldelig *rettsvillfarelse*. Hvis kunden burde ha forstått at det var svindlere som tok kontakt, kan vedkommende vanskelig høres med at det var unnskyldelig å oppgi sikkerhetsinformasjon i strid med utstedelsesavtalen – kunden måtte da ha forstått at det var fare for misbruk. På den annen side vil en faktisk villfarelse forsterke rettsvillfarelsen. Det er av den grunn viktig å behandle villfarelse utførlig når en står overfor en svindelsituasjon, da dette vil kunne ha stor betydning for skyldvurderingen.

4.4 Forsett i utvalgte typetilfeller av ikke godkjente betalingstransaksjoner

4.4.1 Vishing – tilfeller der kunden blir oppringt og oppgir sikkerhetsinformasjon

Vishing inneholder i stor grad de samme elementene som phishing, se punkt 3.5.2. Forskjellen er at kunden har blitt lurt til å oppgi sikkerhetsinformasjon til en svindler som har tatt telefonisk kontakt. Kunden taster altså ikke inn slik informasjon på en narreside, men oppgir denne informasjonen direkte til svindleren. Dette typetilfellet behandles under kapittelet om forsett ettersom praksis etter finansavtaleloven (1999) antyder at å falle for slik svindel etter omstendighetene kan utgjøre et forsettlig pliktbrudd. Dette skillet mellom phishing og vishing kan virke kunstig. Hvis kunden istedenfor å oppgi slik informasjon direkte til svindleren blir dirigert til en narreside ville tilfellet blitt behandlet slik som phishing.[153]

Argumentasjonen for at kunden har handlet forsettlig er gjerne at vedkommende i strid med utstedelsesavtalen bevisst har oppgitt eller overlatt sikkerhetsinformasjon til svindleren. Domstolene har kun ved ett tilfelle behandlet en slik sak, nemlig i nylig avsagte TGLOM-2020-156504.[154] Saken gjaldt såkalt Olga-svindel, hvor en eldre kvinne ble oppringt av en svindler som utga seg for å være fra banken hennes. Kunden ble forledet til å tro at hun

[153] Eksempelvis FinKN-2014-526.

[154] Avgjørelsen er anket og dermed ikke rettskraftig.

hadde tatt opp et lån, og oppga personnummer og passordet til sin BankID gjentatte ganger for å stoppe det som for hun fremsto som en reell utbetaling av et lån. Tingretten mente at kunden i strid med utstedelsesavtalen hadde oppgitt passordet til sin BankID, og ettersom kunden var klar over hva hun gjorde og av egen vilje oppga denne informasjonen, anså retten at pliktbruddet var forsettlig. Tingretten mente videre at det ikke kunne være tale om en unnskyldelig rettsvillfarelse, ettersom det etter rettens oppfatning ikke kunne regnes som unnskyldelig at man har latt være å sette seg inn i kontraktsforpliktelsene. Tingretten anså det tilstrekkelig at kunden bevisst handlet i strid med utstedelsesavtalen, slik også Finansklagenemnda har lagt til grunn.[155] I de tilfellene nemnda har konkludert med at det ikke foreligger forsett, har de ment at det forelå en unnskyldelig rettsvillfarelse, eksempelvis ovennevnte FinKN-2020-707.[156]

Av forarbeidene til finansavtaleloven (2020) følger det imidlertid uttrykkelig at «de foreslåtte endringene innebærer 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».[157] Dette er fordi det ved vurderingen av forsett etter finansavtaleloven (2020) i tillegg kreves at kunden «måtte forstå» at det forelå en «nærliggende fare» for misbruk, se punkt 4.2.2. Vurderingen av hva kunden «måtte forstå» må i hovedsak baseres på de samme elementene som ved phishing, hvor det sentrale vil være *hvem* som tar kontakt og *hva* det er de ber om.

Vurderingen vil også påvirkes av om svindleren utgir seg å være en aktør hvor det er vanlig å oppgi sikkerhetsinformasjon. Eksempelvis vil det på den side være mindre betenkelig å oppgi sikkerhetsinformasjon til sin egen bank, ettersom det for den alminnelige bankkunde vil fremstå som usannsynlig at ens egen bank vil svindle dem. På den annen side vil det være mer betenkelig å oppgi slik informasjon til aktører hvor dette ikke er vanlig – eksempelvis aktører som utgir seg for å være «tech-support».[158]

Det kan være svært vanskelig å avsløre at en henvendelse er reell. Et nummersøk vil ikke nødvendigvis hjelpe kunden, ettersom svindlere som nevnt i punkt 4.3 kan manipulere nummeret som ringer slik at det fremstår som et annet. Henvendelsens innhold vil da være sentralt ved skyldvurderingen. Dersom svindleren utgir seg for å være kundens bank, er dette ofte for å lure kunden til å tro at et lån blir utbetalt. Under det tidspresset kunden opplever, kan det fremstå som rasjonelt at BankID-passordet oppgis for å få stanset utbetalingen av lånet. Slik som ved alminnelig innlogging på nettbanken, har dette karakter av å være en måte å identifisere

[155] Eksempelvis FinKN-2021-156.

[156] Og FinKN-2020-703, FinKN-2020-706 eller FinKN-2021-155.

[157] Innst. L 104 (2020-2021) s. 22.

[158] Eksempelvis FinKN-2021-156, hvor svindleren utga seg for å være fra Microsoft, og nemnda enstemmig kom til at kunden hadde handlet forsettlig.

seg overfor banken på. Dersom kunden bes om å oppgi dette flere ganger, kan det imidlertid være en indikasjon på at det er tale om svindel. Etter omstendighetene vil antallet ganger det bes om at passord og engangskode oppgis kunne innebære at kunden «måtte forstå» at det var nærliggende fare for misbruk.

Dersom kontakten fremstår som om den er fra en reell aktør, og det ikke foreligger grunn til å reagere på innholdet i henvendelsen, vil det heller ikke kunne være tale om en situasjon hvor kunden «måtte forstå» faren for misbruk. Dette vil være i overenstemmelse med slik forsettkravet er praktisert i eksempelvis Danmark, som forarbeidene henviser til. I sak 373/2019, som gjaldt et tilfelle der kunden ble kontaktet av en som utga seg for å være fra betalingstjenestetilbyderen Nets, kom det Finansielle Ankenævn til at kunden ikke hadde handlet forsettlig. Dette til tross for at kunden under samtalen fattet noe mistanke og spurte hvordan han kunne være sikker på at det ikke var tale om svindel, og til tross for at det fremgikk av SMS-ene kunden fikk for å bekrefte betalingstransaksjonene at koden aldri måtte oppgis til tredjemann. Det avgjørende for Ankenævnet var at kunden hadde blitt villedet til å tro at det var en reell henvendelse, og dette utelukket dermed forsett.[159] Ankenævnet konkluderte med at kunden hadde handlet grovt uaktsomt.[160]

Tilsvarende gjelder i Sverige. Sak 2017-13660 fra den svenske Allmänna reklamationsnämnden gjaldt en kunde som i en telefonsamtale ble lurt til å legitimere seg gjennom BankID, og svindleren tappet kundens konto for 140 000 kroner. Nemnda kom til at kunden ikke hadde handlet «särskilt klandervärt». Det sentrale var at kunden hadde blitt utsatt for et «förslaget bedrägeri», slik at kunden ikke «förstod att hans användning av BankID:t kunde få så långtgående konsekvenser». Tilfellet ble imidlertid ansett som grovt uaktsomt.[161]

Spørsmålet i slike saker blir dermed hovedsakelig om kunden har handlet grovt uaktsomt. Dette vil i stor grad bero på en vurdering hvor de samme elementene som gjelder ved phishing er til stede, se punkt 3.5.2. Det avgjørende er om kunden har handlet på en slik måte at dette utgjør et markert avvik fra vanlig forsvarlig handlemåte, der kunden er vesentlig mer å klandre enn ved alminnelig uaktsomhet. I likhet med avgjørelsene fra Danmark og Sverige, er det nærliggende å ut fra omstendighetene anse vishing-tilfellene som grovt uaktsomme pliktbrudd. Det er en vesentlig forskjell mellom phishing og vishing i form av at kunden ved vishing oppgir innloggingsinformasjon på telefon, i motsetning til å selv taste dette inn i på en narreside. Sistnevnte innebærer at kunden bruker passord og betalingsinstrument slik man vanligvis ville

[159] Sml. punkt 4.3 om villfarelse.

[160] Tilsvarende i sakene 294/2020, 285/2020 og 170/2020.

[161] Tilfellet ble behandlet forent med sak 2017-07814.

gjort. Det å oppgi denne informasjonen til en tredjeperson på telefon ligger ikke innenfor det alminnelige bruksområdet til verken BankID eller bankkort.

4.4.2 PIN-kode og betalingsinstrument misbrukes av tredjeperson

Forsettlige pliktbrudd kan også forekomme i tilfeller der kunden fysisk utstyrer en tredjeperson med muligheten til å misbruke kundens betalingsinstrument. Ettersom kunnskap om personlig sikkerhetsinformasjon ifølge forarbeidene ikke alene er tilstrekkelig for å kunne misbruke betalingsinstrumentet, vil det at kunden deler slik informasjon ikke alene medføre ansvar i form av forsett.[162] Det må foreligge konkrete omstendigheter utover dette for at kunden «måtte forstå» at misbruk kunne skje.

Saksforholdet i FinKN-2019-986 er illustrerende. Kunden skulle kjøpe et nettbrett på ferie i Spania, hvor en av de ansatte ville vise framgangsmåten for å bruke betalingsterminalen. På grunn av angivelige problemer med terminalen, gikk kunden for å ta ut penger på en minibank hvor også en av de ansatte var med. Kunden ga både PIN-koden og kortet til den ansatte, og dagen etterpå ble det gjennomført en rekke transaksjoner som kunden ikke vedkjente seg. Nemnda kom til at det var et bevisst pliktbrudd å avsløre koden, som var tilstrekkelig for skyld i form av forsett. Etter ny finansavtalelov blir spørsmålet i tillegg om kunden «måtte forstå» at det var en fare for misbruk.

Det er flere elementer ved en slik situasjon som vil være påfallende. Kunden har ikke bare overgitt koden, men også selve betalingsinstrumentet. I tillegg vil det at en butikkansatt vil vise hvordan man gjennomfører betalingen, og blir med på et kontantuttak, være tilleggsmomenter som ytterligere er egnet til å gi mistanke om potensiell misbruk. Kunden har altså utstyrt den ansatte med alt som er nødvendig for å bruke betalingsinstrumentet, og at dette skjer i et fremmed land under omstendigheter som virker svært unaturlige, er det nærliggende å anse tilfellet slik at det fremstår som uforståelig at kunden var uvitende om faren for misbruk. Lignende tilfeller vil nok anses som forsettlige pliktbrudd også etter finansavtaleloven (2020).

Noen situasjoner gjør det imidlertid nødvendig å dele kode og betalingsinstrument med nærstående eller andre kjente, eksempelvis der man trenger hjelp til å betale regninger eller handle dagligvarer på grunn av svekket helse eller alderdom. Et slik tilfelle var til behandling i FinKN-2016-496 og FinKN-2016-495. Begge sakene gjaldt det samme saksforholdet, og må leses i sammenheng. Førstnevnte sak gjaldt kundens debetkort, mens sistnevnte sak gjaldt kundens kredittkort. Begge kortene hadde samme forhåndsbestemte kode. Kunden, som på grunn av hjertesykdom trengte hjelp til å handle, ga debetkortet og kode til sitt barnebarn.

[162] Innst. 104 L (2020-2021) s. 21-22.

Ettersom disse var bevisst overlatt til en tredjeperson, kom nemnda i FinKN-2016-496 til at pliktbruddet var forsettlig.

Forholdet hadde imidlertid vært bedømt annerledes etter finansavtaleloven (2020). Ettersom kunden var syk, var det tale om en situasjon hvor hun var avhengig av hjelp for å få gjennomført dagligvarehandelen. Det er nettopp i disse situasjonene at forarbeidene forutsetter at vilkåret om forsett ikke er oppfylt. Dersom det forelå ytterligere omstendigheter som var egnet til å gi kunden mistanke om at misbruk kunne skje, eksempelvis at barnebarnet hadde misbrukt kortet før, eller at barnebarnet tidligere har utvist «forbrytersk forsett» som var egnet til å betvile deres hensikt,[163] ville tilfellet lettere vært bedømt som et forsettlig pliktbrudd. Dette var imidlertid ikke situasjonen i denne saken, og utover det faktum at kort og kode ble delt med barnebarnet, forelå det ingen andre omstendigheter som skulle tilsi at misbruk av betalingsinstrument var en fare. Av den grunn kan det heller ikke sies at det forelå noen rimelig grunn til å være uvitende om at dette kunne skje, og forholdet hadde neppe vært bedømt som et forsettlig pliktbrudd etter finansavtaleloven (2020).

Det danske Finansielle Ankenævn avgjorde et lignende tilfelle i sak 146/2008, der en kunde som var innlagt på sykehus trengte hjelp til et kontantuttak og oppga kode og kort til en venn som senere misbrukte kortet. Ankenævnet mente at kunden «burde have fået mistanke om en sådan risiko» for misbruk da vennen ikke leverte tilbake kortet som avtalt, men at kunden ikke burde ha fattet slik mistanke da kortet og koden ble avlevert til vennen. På det tidspunktet forelå det ingen konkrete omstendigheter som tilsa at det var fare for misbruk, og Ankenævnet utelukket av den grunn at det var tale om et forsettlig pliktbrudd.

Gode grunner taler for at ovennevnte sak fra Finansklagenemnda ville fått et lignende utfall etter finansavtaleloven (2020). Både eksemplifiseringen av lignende situasjoner i forarbeidene, og hensynet bak implementeringen av vilkåret om at kunden «måtte forstå» at det var en nærliggende fare for misbruk, tilsier dette.

4.5 Sammenfatning

Finansavtaleloven (2020) presiserer vurderingstemaet for forsett ved ikke godkjente betalingstransaksjoner. Ansvarsbegrensningene i § 4-30 bortfaller i sin helhet dersom kunden «forsettlig» har misligholdt sine plikter, og i tillegg «måtte forstå» at pliktbruddet kunne innebære en «nærliggende fare» for misbruk. I dette ligger det at pliktbruddet må være bevisst og at det etter en normal bedømmelse av situasjonen fremstår som uforståelig at kunden var uvitende om faren for misbruk.

[163] Sml. BKN-2007-150.

Lovgiver har tatt et klart standpunkt at dersom kunden har behov for hjelp til nødvendige gjøremål, så vil ikke ansvarsbegrensningene bortfalle kun ved at kunden deler kode eller passord med en tredjeperson. Dette i motsetning til hvordan forsettkravet er forstått i tidligere utgaver av finansavtaleloven, se punkt 4.2.1. Presiseringen av forsettkravet i finansavtaleloven (2020) medfører dermed en endring i hva som utgjør forsettlige pliktbrudd i de tilfellene kunden utstyrer en tredjeperson med muligheten til å bruke betalingsinstrumentet. Slik gjennomgangen av typetilfellene i punkt 4.2.2 viser, vil kunden også i større grad være beskyttet av ansvarsbegrensningene i § 4-30 i de tilfellene man blir fralurt informasjon om betalingsinstrumentet og tilhørende kode. Hvorvidt det foreligger et forsettlig pliktbrudd som medfører at ansvarsbegrensningene bortfaller, vil i større grad måtte bero på en konkret vurdering av forholdene i den individuelle saken. Dersom kunden har blitt utsatt for vishing, medfører lovendringen at aktsomhetsvurderingen i større grad vil tilsvare den i phishing-tilfellene. Dette vil harmonere godt med hvordan kundens skyld er vurdert i både Sverige og Danmark i tilsvarende saker.

5 Avslutning

Sikre og trygge betalingstjenester er en forutsetning for et velfungerende betalingstjenestemarked, og et av de sentrale formålene med PSD 2 er å sørge for at forbrukere er tilstrekkelig beskyttet mot den økende risikoen som medfølger elektroniske betalingsløsninger.[164] Av den grunn må også ansvarsfordelingen mellom betalingstjenesteyteren og kunden innebære at tillitten til slike betalingsløsninger styrkes. EU-kommisjonen har understreket at det digitale indre markedet skal sikre EU-borgere samme sikkerhetsnivå og de samme forventninger som i hverdagen utenfor den digitale verden.[165] Praktiseringen av skyldreglene, i kombinasjon med de sofistikerte svindelmetodene som utnytter svakheter ved digitale betalingstjenester, er egnet til å skape tvil om at det oppleves like trygt å ferdes digitalt som analogt.

Svindel er ikke et nytt fenomen. Kundens betalingsinstrument og kode kan stjeles og signaturer kan forfalskes. I de sistnevnte tilfellene er imidlertid kunden beskyttet av de ulovfestede avtalerettslige reglene om falsk, som utgjør en sterk ugyldighetsgrunn.[166] Kunden kan da som utgangspunkt ikke holdes ansvarlig for det økonomiske tapet. Av den grunn kan det også påstås at digitaliseringen av betalingstjenester har medført et skifte i hvordan risikoen fordeles mellom kunden og betalingstjenesteyteren når svindel har funnet sted.[167] Et betimelig spørsmål er da om finansinstitusjonene bør ta en større del av risikoen ved ikke godkjente betalingstransaksjoner?

Finansavtaleloven (2020) endrer ikke risikofordelingen som sådan, utover at kunden holdes ansvarlig for en mindre objektiv egenandel enn etter gjeldende finansavtalelov. Avhandlingen har vist at det er uenighet om innholdet i det kontraktsrettslige forsettbegrepet, men ny finansavtalelov presiserer innholdet i dette på området for finansielle tjenester, som styrker kundens forutberegnelighet og posisjon i tilfeller hvor betalingstjenesteyteren påberoper seg et forsettlig pliktbrudd. Avhandlingen har også vist at praktiseringen av grensen for grov uaktsomhet til tider, og særlig ved phishing, har vært såpass streng at det er grunnlag for å betvile om grensen er praktisert i tråd med Høyesteretts forutsetninger.

Dette bringer oss til kjernen av problemet: vurderingen av om ansvarfordelingen mellom kunden og betalingstjenesteyteren er rimelig og hensiktsmessig, vil hovedsakelig bero på hvordan skyldgrensene praktiseres. Utgangspunktet er klart: kundene nyter et godt vern dersom deres betalingsinstrumenter blir misbrukt, der kunden er beskyttet av en etter omstendighetene

[164] Fortalen til PSD 2 punkt 7.
[165] SWD (2019) 192 s. 51.
[166] Giertsen (2014) s. 170.
[167] Kjørven (2020) s. 104.

lav egenandel. Det er først ved den groveste form for skyld at de lovfestede ansvarsbegrensningene bortfaller. Dersom skyldgrensene imidlertid ikke praktiseres slik at det gjenspeiler hvordan den alminnelige bankkunde håndterer betalingsinstrumenter, vil dette gå utover både tillitten til slike betalingsløsninger og kundens forutberegnelighet. Dette vil gå på akkord med selve formålet med regelverket.

Det er i stor grad behov for en endring av hvordan grensen for grov uaktsomhet ved enkelte tilfeller praktiseres. Dette kan imidlertid ikke alene begrunne at risikoen er skjevfordelt. For å bøte på en til tider nokså vilkårlig praksis, og for å forsikre en harmonisert forståelse skyldreglene i PSD 2, er det langt på vei nødvendig med en avklaring på hva som nærmere ligger i *direktivets* skyldbegreper.[168] All den tid direktivet hviler på udefinerte skylbegreper, legges det opp til at nasjonale rettstradisjoner vil medføre en sprikende praksis på tvers av landegrensene – særlig dersom stadig nye svindelmetoder dukker opp.

Til tross for dette, er det på dette tidspunkt neppe grunnlag for å kunne trekke en slutning om at risikoen er skjevfordelt, og at betalingstjenesteyteren av den grunn burde ta en større del av ansvaret når misbruk først skjer. Hvis praksis derimot viser seg å gå for langt i å pålegge kunden en større egenandel, eller skyldkravene praktiseres i strid med hensikten bak lovendringen, vil det være høyst aktuelt å diskutere en endring i ansvarsfordelingen. Dette vil bero på om reglene etter finansavtaleloven (2020) praktiseres på en rimelig og hensiktsmessig måte, noe vi først vil finne ut av etter at loven trer i kraft.

[168] Kjørven (2020) s. 106.

Kildeliste

LITTERATUR:

Andenæs (2009) — Andenæs, Mads Henry. *Rettskildelære*. 2. utg., Oslo: M.H. Andenæs, 2009.

Andenæs (2016) — Andenæs, Johs. *Alminnelig strafferett*. 6. utg., ved Georg Fredrik Rieber-Mohn og Knut Erik Sæther, Oslo: Universitetsforl., 2016.

Arnholm (1973) — Arnholm, Carl Jacob. *Almindelig obligasjonsrett*. 2 utg., Oslo: Tanum-Norli, 1973.

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

Bergo (2019) — Bergo, Knut. «Tolkning og anvendelse av lov, forskrift og forarbeider». I *Juridisk metode og tenkemåte*. Alf Petter Høgberg og Jørn Øyrehagen Sunde red., Oslo: Universitetsforlaget, 2019, s. 176-238.

Bruserud (2010) — Bruserud, Herman. *Hardshipklausuler*. Bergen: Fagbokforl., 2010.

Bruserud (2011) — Bruserud, Herman. «Villfarelse om ugyldighets- og forpliktelsesgrunnlag». *Marius* nr. 401 (2011).

Falkanger (1997) — Falkanger, Aage Thor. «Erstatningsansvar der skyldneren har misligholdt pga villfarelse om det rettslige innholdet i sin kontraktsforpliktelse». I *Fra institutt til fakultet: jubileumsskrift i anledning av at IRV ved Universitetet i Tromsø feirer 10 år og er blitt til Det juridiske fakultet*. Jens Edvin A. Skoghøy red., Oslo: Pensumtjeneste.

Fredriksen og Mathisen (2018) — Fredriksen, Halvard Haukeland og Gjermund Mathisen. *EØS-rett*. 3. utg., Bergen: Fagbokforl., 2018.

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

Giertsen (2019) — Giertsen, Johan. *Kontrakter: ytelse og pris*. Oslo: Universitetsforl., 2019.

Grøttjord og Rosén (2014) — Grøttjord, Børge og Karl Rosén. *Finansavtaleloven: med kommentarer*. Oslo: Gyldendal, 2014.

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

Hagstrøm og Stenvik (2019) — Hagstrøm, Viggo og Are Stenvik. *Erstatningsrett*. 2. utg., Oslo: Universitetsforl., 2019.

Hallsteinsen (2018) — Hallsteinsen, Peter. *Alminnelig obligasjonsrett*. Oslo: Gyldendal, 2018.

Kaasen (2005) — Kaasen, Knut. «Ansvarsbegrensninger i fabrikasjonskontrakter». I *Industribygging og rettsutvikling: juridisk festskrift i anledning Hydros 100-årsjubileum*. Odd Ivar Biller red., Bergen: Fagbokforl., 2005, s. 233-258.

Kjelland (2019) — Kjelland, Morten. *Erstatningsrett: en lærebok*. 2. utg., Oslo: Universitetsforl., 2019.

Kjørven (2020) — Kjørven, Marte E. «Who pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe». *European Business Law Review* årg. 31, nr. 1 (2020) s. 77-109.

Krüger (1968) — Krüger, Kai. «Om forsett i privatretten – særlig om det forsettlige mislighold». *Jussens venner* årg. 3 nr. 2 (1968) s. 43-79.

Krüger (1989) — Krüger, Kai. *Norsk kontraktsrett*. Bergen: Alma Mater forl., 1989.

Lund (1970) — Lund, Ketil. «Bemerkninger om noen hovedpunkter i læren om villfarelse». *Jussens venner* årg. 5 nr. 2 (1970) s. 57-94.

Mæhle og Aarli (2019) — Mæhle, Synne Sæther og Ragna Aarli. «Juridisk metode for morgendagens jurister». I *Juridisk metode og tenkemåte*. Alf Petter Høgberg og Jørn Øyrehagen Sunde red., Oslo: Universitetsforlaget, s. 114-134.

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

Skoghøy (2018) — Skoghøy, Jens Edvin A. *Rett og rettsanvendelse*. Oslo: Universitetsforl., 2018.

Sejersted (2011) — Sejersted, Fredrik mfl. *EØS-rett*. 3. utg., Oslo: Universitetsforl., 2011.

Wilhelmsen og Hagland (2017) — Wilhelmsen, Trine-Lise og Birgitte Hagland. *Om erstatningsrett: med utgangspunkt i tekster av Peter Lødrup*. Oslo: Gyldendal, 2017.

Woxholth (2017) — Woxholth, Geir. *Avtalerett*. 10. utg., Oslo: Gyldendal, 2017.

NORSKE RETTSKILDER:

Lover

1918 — Lov av 31. mai 1918 nr. 4 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer (avtaleloven).

1961 — Lov av 3. februar 1961 om ansvar for skade som motorvogner gjer (bilansvarslova).

1985 — Lov av 21. juni 1985 om kredittkjøp m.m. (kredittkjøploven).

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

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

1999 — Lov av 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven).

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

Forarbeider

NOU 1994:19 *Finansavtaler og finansoppdrag. Delutredning nr. 1.*

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.*

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 fra justiskomiteen om Lov om finansavtaler (finansavtaleloven).*

Lovvedtak 24 (2020-2021) *Lov om finansavtaler (finansavtaleloven).*

Meld. St. 31 (2020-2021) *Finansmarkedsmeldingen 2021.*

Rettspraksis

Rt. 1978 s. 321.
Rt. 1984 s. 248.
Rt. 1987 s. 744.
Rt. 1995 s. 1350.
Rt. 2002 s. 696.
Rt. 2002 s. 1110.
Rt. 2004 s. 499.
HR-2020-1262-A.
HR-2020-2021-A.
HR-2020-2401-A.

LB-2016-43622.

TGLOM-2020-156504.

Nemndspraksis

Transportklagenemnda Fly:

FLYKN-2017-3300.
FLYKN-2018-2518.
FLYKN-2019-145.

Finansklagenemnda og Bankklagenemnda:

BKN-1995-47.
BKN-2005-163.
BKN-2006-127.
BKN-2007-125.
BKN-2007-150.
BKN-2008-81.
BKN-2009-6.

FinKN-2013-276.
FinKN-2014-526.
FinKN-2014-528.
FinKN-2016-495.
FinKN-2016-496.
FinKN 2017-580.
FinKN-2017-649.
FinKN-2018-46.
FinKN 2018-311.
FinKN-2018-530.
FinKN-2019-40.
FinKN-2019-336.
FinKN-2019-338.
FinKN-2019-565.
FinKN-2019-681.
FinKN-2019-683.
FinKN-2019-986.
FinKN-2020-52.
FinKN-2020-230.
FinKN-2020-455.

FinKN-2020-703.
FinKN-2020-706.
FinKN-2020-707.
FinKN-2021-107.
FinKN-2021-155.
FinKN-2021-156.

INTERNASJONALE RETTSKILDER:

Traktater og EU-rettsakter

EØS-avtalen	*Avtale om Det europeiske økonomiske samarbeide*, Oporto, 2. mai 1992. [Offisiell norsk oversettelse].
Direktiv 93/13/EØF	*Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler* [Forbrukeravtaledirektivet].
Direktiv 2007/64/EF	*Europa-Parlamentets og Rådets direktiv 2007/64/EF af 13. november 2007 om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF* [Betalingstjenestedirektivet, PSD 1]
Direktiv (EU) 2015/2366	*Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF* [Betalingstjenestedirektivet, PSD 2]
Forordning (EU) 2018/389	*Kommissionens delegerede forordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation*.

Rettspraksis fra EU-domstolen

Sag C-616/11 T-mobile Austria GmbH mod Veren für Konsumenteninformation	ECLI:EU:C:2014:242

Sag C-26/13 Kásler og Rábai mod OTP Jelzálogbank Zrt	ECLI:EU:C:2014:282
Sag C-186/16 Andriciuc m.fl. mod Banca Românească SA	ECLI:EU:C:2017:703
Sag C-287/19 DenizBank AG mod Verein für Konsumenteninformation	ECLI:EU:C:2020:897

Forarbeider

SWD (2015) 100	*A Digital Single Market Strategy for Europe – Analysis and Evidence*.

<u>UTENLANDSKE RETTSKILDER:</u>

Lover

Betaltjänstlagen	Lag (2010:751) om betaltjänster [Sverige].
Betalingsloven	Lov nr. 652 af 8. juni 2017 om betalinger [Danmark].

Praksis fra det danske Finansielle Ankenævn

Sag 146/2008.
Sag 290/2018.
Sag 373/2019.
Sag 294/2020.
Sag 285/2020.
Sag 170/2020.

Praksis fra det svenske Allmänna Reklamationsnämnden

Beslut 2017-07814.
Beslut 2017-13660.

Praksis fra den britiske Financial Ombudsman Service

DRN-4773354, avsagt 21. desember 2018.
DRN-5688949, avsagt 26. april 2019.
DRN-4139348, avsagt 2. juli 2020.
DRN-2174713, avsagt 15. september 2020.
DRN-4082710, avsagt 22. desember 2020.

AVTALER OG REGELVERK:

Finansklagenemnda, avtale — «Avtale om Finansklagenemnda mellom Forbrukerrådet, Finans Norge, Næringslivets Hovedorganisasjon, Finansieringsselskapenes forening, Verdipapirfondenes forening og Virke», sist revidert 28.09.2016. https://www.finkn.no/Om-oss/Regelverk/Avtale-om-Finansklagenemnda [hentet 21. januar 2021].

Finansklagenemnda, vedtekter — «Vedtekter for Finansklagenemnda», sist revidert, 23.11.2018. https://www.finkn.no/Om-oss/Regelverk/Vedtekter-for-Finansklagenemnda [hentet 21. januar 2021].

Næringslivets Konkurranseutvalg — «Vedtekter for Næringslivets Konkurranseutvalg», sist endret 03.04.2017. http://konkurranseutvalget.no/vedtekter/ [hentet 21. januar 2021].

PUBLIKASJONER OG NETTSIDER:

Finanstilsynet (2020) — Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2020*. Oslo: 14. mai 2020. https://www.finanstilsynet.no/contentassets/816cd5c4576a484ab41749a3ff985a69/risiko--og-sarbarhetsanalyse-2020.pdf [hentet 18. januar 2021].

Finanstilsynet (2021) — Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2021*. Oslo: 12. mai 2021. https://finanstilsynet.no/contentassets/98a84484055840fc8bfd0cb7b78dd025/ros-2021.pdf [hentet 16. mai 2021]

Forbrukertilsynet (2017) — Forbrukertilsynet. «Advarer mot e-postsvindel» (28. mars 2017) https://www.forbrukertilsynet.no/advarer-e-postsvindel [hentet 15. mars 2021].

Nissen (2021) — Nissen, Sofie Grønntun mfl., «Oslo kommune vil at de som ønsker vaksine, skal registrere seg digitalt. For

mange kan det være en komplisert prosess». *Aftenposten*, 19. februar 2021, https://www.aftenposten.no/norge/i/dlkagw/oslo-kommune-vil-at-de-som-oensker-vaksine-skal-registrere-seg-digital [hentet 15. mars 2021].

Norges Bank (2020) — Norges Bank. *Kunderetta betalingsformidling 2019*. Norges Bank Memo 1/2020. Oslo: 19. mai 2020. https://static.norges-bank.no/contentassets/b5b8151d59fe48b3bae68b6e5cb99971/memo_1_20_notat.pdf?v=05/18/2020163620&ft=.pdf [hentet 18. januar 2021].

NorSIS (2020) — Norsk senter for informasjonssikring. *Få en tryggere digital hverdag: Trusler og trenger 2019-2020.* Gjøvik: 2020. Kan lastes ned her: https://norsis.no/publikasjoner/ [hentet 4. februar 2021].

Næringslivets sikkerhetsråd (2020) — Næringslivets sikkerhetsråd. *Mørketallsundersøkelsen 2020*. Oslo: 7. september 2020. https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2020-web.pdf [hentet. 22. januar 2021].

Regjeringen (2020) — Regjeringen. «Offisielt frå statsrådet 18. desember 2020». (18. desember 2020) https://www.regjeringen.no/no/aktuelt/offisielt-fra-statsradet-18.-desember-2020/id2815084/ [hentet 18. januar 2021].