Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Tapsfordeling mellom bank og kunde ved misbruk av elektroniske betalingsinstrumenter – når har kunden opptrådt grovt uaktsomt?

Forfatter: Habibija, Admir

Publiseringsdato: 6. juni 2023
Publisert av: Karnov forlag
Inngår i artikkelsamling: Bruk og misbruk av elektronisk identifikasjon – ISBN 978-82-93816-31-7
Lenke til hele publikasjonen i Lovdata Pro: https://lovdata.no/pro/KARNOV/karnov-2022-03

Fagfellevurdert artikkel

Artikkelen ble publisert 6. juni 2023. Kilder det er lenket til, kan senere ha blitt erstattet eller fjernet.

1 Innledning[1]

De siste tiårene har betalingssystemet i Norge blitt nærmest heldigitalisert. Betalingskort har erstattet kontanter, og digitaliseringen har bidratt til en gradvis utfasing av den fysiske banken. Overgangen til elektroniske betalingsløsninger innebærer store effektivitetsgevinster, men fører samtidig med seg økt risiko for svindel. I 2021 ble det i Norge rapportert om tap knyttet til misbruk av betalingskort tilsvarende 159,3 millioner kroner og tap knyttet til nettbanksvindel tilsvarende 346 millioner kroner.[2]

Tredjepersons misbruk av betalingsinstrument og tilhørende kode eller passord, og særlig såkalt *phishing*, er blant de vanligste tilfellene av misbruk av

[1] Artikkelen er en omarbeidet versjon av min masteroppgave, som ble ferdigstilt våren 2021, og som ble til under verdifull veiledning fra professor Marte Eidsand Kjørven. Artikkelen er skrevet etter råd og innspill fra redaktørene, dyktige kollegaer i advokatfirma DLA Piper, fagfelle og venner. En stor takk til alle.

[2] Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2022*, Finanstilsynet, 2022, s. 35–39.

betalingsinstrumenter i Norge[3] og i Europa.[4] «Phishing» er en form for sosial manipulering, hvor svindleren spiller på fristelser, frykt, tillit og/eller en opplevelse av tidspress for å «fiske» etter informasjon om et betalingsinstrument og personlig sikkerhetsinformasjon. Vanligvis skjer dette gjennom en e-post eller tekstmelding som er lik eller identisk med en reell melding fra en institusjon man har tillit til, eksempelvis egen bank eller offentlige institusjoner.[5] E-posten eller sms-en inneholder en lenke til en falsk nettside som ser ut som eksempelvis innloggingssiden til svindelofferets nettbank eller Skatteetatens nettsider. Dersom offeret legger inn sikkerhetsinformasjon på nettsiden i et forsøk på å logge seg inn, vil svindleren kunne bruke denne informasjonen til å logge seg på den reelle nettbanken og tømme offerets konto.

En særlig form for phishing er «voice phishing» eller «vishing», hvor svindleren tar telefonisk kontakt med offeret. De mye omtalte «Olga-sakene», hvor eldre personer blir oppringt av svindlere og fralurt BankID-informasjon, er eksempler på «vishing».[6]

Det kan også utgjøre en risiko for svindel dersom kunden skriver ned passord og PIN-koder og oppbevarer disse lett tilgjengelig for nærstående eller andre tredjepersoner. Kunden kan også oppgi sikkerhetsinformasjon frivillig til tredjepersoner, for eksempel for å få hjelp til betale regninger.

Svindleren vil naturligvis alltid være økonomisk ansvarlig for tapet. Fordi det ofte er vanskelig å finne svindleren og holde ham eller henne ansvarlig, blir spørsmålet i praksis ofte om det er kunden (kontohaveren) eller betalingstjenesteyteren (banken) som skal bære tapet. Ansvarsfordelingen mellom bank og kunde ved ikke godkjente betalingstransaksjoner var i hovedsak ulovfestet frem til vedtakelsen av finansavtaleloven (1999).[7] Unntaket var kredittkort, som var regulert av kredittkjøpsloven av 1985.[8] Etter kredittkjøpsloven § 13 var kunden som hovedregel ansvarlig for hele tapet ved utvist ved forsett eller grov uaktsomhet og for en egenandel på 500 kroner ved uaktsomhet. Utenom disse tilfellene fulgte risikoplasseringen av finansinstitusjonenes standardkontrakter. Den manglende lovreguleringen innebar at tapet ble plassert hos kunden allerede ved simpel uaktsomhet.[9] Før kredittkjøpsloven var ansvarsfordelingen i

---

[3] Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2022*, Finanstilsynet, 2022, s. 35 flg.

[4] European Payments Council. European Payments Council. *2021 payment threats and fraud trends report*. Brussel, 2021, s. 14 flg. (hentet 1. november 2022)

[5] NorSIS. *Trusler og trender 2021*. NorSIS, 2021. https://norsis.no/publikasjoner/ (hentet 4. november 2022), s. 19.

[6] Se for eksempel saksforholdet i HR-2022-1752-A og nærmere under punkt 7.4.

[7] Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag. Reglene i finansavtaleloven (1999) § 35 gjennomførte regler i PSD 2s forløper, Europaparlaments- og rådsdirektiv 2007/64/EF av 13. november 2007 om betalingstjenester i det indre marked.

[8] Lov 21. juni 1985 nr. 82 om kredittkjøp m.m.

[9] Olav Torvund, «Betalingskort ('Kredittkort') – betalingsinstrumenter på uryddig grunn», *Lov og Rett,* årg. 25, nr. 6, 1986, s. 350.

sin helhet overlatt til kontraktsrettslig regulering. I forarbeidene til kredittkjøpsloven fremhever Kredittkjøpsutvalget at finansinstitusjonene, som den sterke avtalepart, i sine standardkontrakter i praksis la all risiko for misbruk av kredittkort og betalingskort over på kundene.[10]

I dag reguleres ansvarsfordelingen av finansavtaleloven (2020) § 4-30.[11] Bestemmelsen gjennomfører reglene i direktiv (EU) 2015/2366 (PSD 2) om tapsfordeling ved ikke godkjente betalingstransaksjoner.[12] Reglene er i hovedsak en videreføring av tilsvarende regler i finansavtaleloven (1999) § 35.

Hovedregelen etter finansavtaleloven (2020) § 4-30 er at betalingstjenesteyteren er ansvarlig for tap som skyldes en ikke godkjent betalingstransaksjon. Dette objektive ansvaret modereres i de påfølgende leddene. Etter annet ledd svarer kunden på visse vilkår for en egenandel på inntil 450 kroner. Ved misbruk av elektronisk betalingsinstrument svarer kunden for en egenandel på inntil 12 000 kroner dersom tapet skyldes at kunden har opptrådt grovt uaktsomt. Kunden svarer for hele tapet ved forsettlig pliktbrudd og ved grovt uaktsomt pliktbrudd i andre tilfeller enn ved misbruk av elektronisk betalingsinstrument. Grensen mellom de tre tersklene for egenandel har dermed avgjørende betydning for hvor stor del av tapet henholdsvis kunden og banken må bære. Spørsmålet som skal besvares i denne artikkelen, er når kunden har opptrådt «grovt uaktsomt» i finansavtalelovens forstand. Jeg skal i den sammenheng særlig undersøke i hvilken grad typiske forhold som fører til tap – å falle for *phishing*- og *vishing*-angrep samt skrive ned passord eller PIN-kode – innebærer at kunden har opptrådt grovt uaktsomt.[13] Praksis fra Finansklagenemnda viser at dette er typiske tilfeller hvor tvist om tapsfordelingen etter misbruk av elektroniske betalingsinstrumenter finner sted.

I det følgende vil jeg i punkt 2 først gi en oversikt over reguleringen av ikke godkjente betalingstransaksjoner, herunder når en transaksjon er «ikke godkjent». Kundens plikter med hensyn til håndtering av betalingsinstrumentet og kundens varslingsplikt gjennomgås i punkt 3. Deretter behandles det som er artikkelens hovedtema, grensen for grov uaktsomhet, i punktene 4 til 7. Jeg skal først redegjøre for hva som er vurderingstemaet for grovt uaktsomme pliktbrudd i punkt 4. Deretter drøftes særskilt betydningen av kundens individuelle forhold i punkt 5 og betydningen av manglende sikkerhetsrutiner hos betalingstjenesteyteren i punkt 6. I punkt 7 vil jeg nærmere

---

[10] Ot.prp. nr. 34 (1980–81) s. 81.

[11] Lov 18. desember 2020 nr. 146 om finansavtaler. Loven ble vedtatt i desember 2020 og trådte i kraft 1. januar 2023.

[12] Direktivet er med virkning fra 1. mai 2022 inkorporert i EØS-avtalen, se EØS-komiteens beslutning nr. 165/2019 av 14. juni 2019 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester).

[13] Hva som utgjør et forsettlig pliktbrudd på kundens hånd, er grundig analysert av Kjørven, Woxholth og Høgberg og behandles ikke nærmere her. Se Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6 2021, s. 335–366.

undersøke den nedre grensen for hva som utgjør grovt uaktsomme pliktbrudd på kundens hånd, i utvalgte typetilfeller.

Ved fastleggelse av reglene i finansavtaleloven vil de EØS-rettslige rammene som følger av PSD 2, danne et utgangspunkt. Som jeg skal komme tilbake til, åpner imidlertid PSD 2 eksplisitt for at graden av kundens uaktsomhet vurderes i tråd med nasjonal rett.

Høyesterett har i to nylige saker, HR-2020-2021-A og HR-2022-1752-A, behandlet spørsmålet om kundens ansvar for tap etter BankID-svindel. HR-2020-2021-A gjaldt misbruk av elektronisk signatur (BankID) til lånopptak og omhandlet følgelig ikke betalingstransaksjoner. HR-2022-1752-A gjaldt spørsmålet om hvorvidt kunden hadde handlet forsettlig etter finansavtaleloven (1999) § 35 tredje ledd. Ingen av dommene gjelder direkte de spørsmål som skal drøftes i denne artikkelen. De er likevel relevante i denne artikkelen, ettersom Høyesterett i begge sakene går inn på reglene om ikke godkjente betalingstransaksjoner og systemet for ansvarsfordelingen mellom kunde og finansinstitusjon etter finansavtaleloven (1999). I tillegg til disse avgjørelsene har Høyesterett kun ved ett tilfelle, i Rt-2004-499, behandlet spørsmålet om grov uaktsomhet ved ikke godkjente betalingstransaksjoner. Samtlige av disse dommene vil derfor være relevante å behandle nærmere i denne artikkelen.

Videre vil praksis fra Finansklagenemnda brukes til å eksemplifisere de aktuelle svindeltilfellene.[14] Svært få svindelsaker behandles i domstolene, og ofte begynner og slutter saken i Finansklagenemnda. Bakgrunnen for dette er at disse tilfellene i hovedsak har en begrenset tvistesum på opp til 12 000 kroner, og kostnadene ved å føre en sak for domstolene vil i de fleste tilfeller overgå tvistesummen. I praksis innebærer dette at Finansklagenemnda er organet som vil anvende regelverket overfor forbrukere i de aller fleste tilfellene. Gjennomgangen vil vise at den terskelen Finansklagenemnda har anvendt, neppe er i samsvar med gjeldende rett. Nyere praksis tyder imidlertid på at flertallet i nemnda er i ferd med å justere seg. Særlig interessant er en helt fersk avgjørelse fra mars 2023, FinKN-2023-188, som synes å innebære et taktskifte. Dette vil kommenteres nærmere under punkt 7.3. På grunn av tvistesummen i disse sakene vil spørsmålet neppe komme opp for domstolene. Noen rettspolitiske betraktninger rundt dette vil bli drøftet avslutningsvis i punkt 8.

2 Innledende om reguleringen av ikke godkjente betalingstransaksjoner

Helt siden vedtakelsen av finansavtaleloven (1999) har hovedregelen vært at betalingstjenestetilbydere må bære tapet etter ikke godkjente (tidligere kalt

[14] Finansklagenemndas praksis har imidlertid svært begrenset rettskildeverdi. Selv om det er en relevant rettskilde, kan ikke avgjørelsene tillegges noe særlig vekt – selv der praksisen er konsekvent. Se Mads Henry Andenæs, *Rettskildelære*, 2. utg., M.H. Andenæs, 2009, s. 98 og Viggo Hagstrøm mfl., *Obligasjonsrett,* 3. utg. ved Herman Bruserud mfl., Universitetsforlaget, 2021, s. 62.

«uautoriserte») betalingstransaksjoner. Det er samfunnsøkonomiske hensyn som er den bærende begrunnelsen for en slik regel:[15] Det er gunstig for samfunnet å legge til rette for bruk av elektroniske betalingsinstrumenter uten at kundene må påta seg en betydelig økonomisk risiko. Betalingstjenestetilbyderne kan pulverisere tapet og oppfordres samtidig til å utvikle sikre betalingsløsninger. Prevensjonshensyn tilsier på den annen side at kunden bør ha et insentiv til å håndtere betalingsinstrumenter med tilhørende sikkerhetsinformasjon med forsiktighet.

Systemet med økende egenandeler for kunden basert på graden av klander skal balansere disse hensynene. I HR-2022-1752-A avsnitt 35 trekkes disse hensynene frem ved gjennomgangen av systemet i finansavtaleloven (1999) § 35, hvor det ved fravær av et forsettlig pliktbrudd blir understreket at «[g]runnen til at ansvaret for kunden ikkje er uavgrensa i slike høve, er at det er tenleg for bankane og samfunnet å leggje til rette for at kundane nyttar elektroniske betalingsinstrument». Høyesterett fremhever i denne sammenheng at finansinstitusjonene kan pulverisere tapet ved å spre kostnadene på kundemassen.

Det følger av § 4-30 første ledd at banken bare er ansvarlig for tap som skyldes en «ikke godkjent betalingstransaksjon, jf. § 4-2».[16] Det følger videre av § 4-2 første ledd at en betalingstransaksjon er godkjent «bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres».[17] Motsetningsvis vil betalingstransaksjonen være «ikke godkjent» dersom betaleren *ikke* har gitt samtykke til den. 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. Betalingstjenesteyternes standardavtaler for bruk av betalingskort detaljregulerer ikke hvordan samtykke skal gis, men nøyer seg med å henvise til at en betalingstransaksjon er godkjent «bare dersom betaleren har gitt sitt samtykke til betalingstransaksjonen …».[18] Avtaleverket for BankID henviser til reglene i finansavtaleloven.[19] Det følger imidlertid av sammenhengen at samtykke forutsetter at

[15] Ot.prp. nr. 94 (2008–2009) s. 128.

[16] Uttrykket «betalingstransaksjon» er i § 1-5 sjette ledd definert som «en handling som iverksettes av betaleren eller på dennes vegne eller av betalingsmottakeren for å innbetale, overføre eller ta ut betalingsmidler …», jf. også PSD 2 artikkel 4 nr. 5.

[17] Tilsvarende Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked artikkel 64.

[18] DNB. «Avtalevilkår for BankAxept/Visa/Mastercard betalingskort og andre kortbaserte betalingsinstrumenter (debet) – forbruker». 2023. (hentet 31. mars 2023). Avtalevilkårene kan variere fra bank til bank, men følger i stor grad samme standard.

[19] DNB. «Avtale om BankID». (u.å). (hentet 31. mars 2023) etter standard fra BITS.

det er *kunden* som må ha bekreftet betalingen med personlig kode eller annen personlig sikkerhetsanordning.[20]

Forarbeidene til finansavtaleloven (2020) slår fast at § 4-2 viderefører det som da var 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».[21] 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 bestemmelsene om ugyldige viljeserklæringer i avtaleloven,[22] supplert av ulovfestede ugyldighetsregler, inkludert falsk.[23]

Et særlig spørsmål oppstår i de tilfellene der kunden blir lurt til selv å gjennomføre betalingstransaksjonen, eksempelvis ved såkalt kjærlighetssvindel, hvor kunden overfører penger til en annen person i den tro at vedkommende har funnet kjærligheten. Et annet eksempel er fakturasvindel, hvor kunden gjennomfører en betaling basert på en forfalsket faktura.

Fellesnevneren for de ovennevnte tilfellene er at det er kunden selv som utsteder betalingsordren. Betalingstjenesteyteren er etter § 4-28 første ledd ansvarlig overfor betaleren for «korrekt gjennomføring» av en betalingstransaksjon som iverksettes av betaleren.[24] Betalingstransaksjonen er korrekt gjennomført når betalingsoppdraget gjelder en betalingsmottaker som det angitte kontonummeret eller annen entydig identifikasjon utpeker, jf. § 4-26 første ledd.[25] Betalingstjenesteyteren trenger følgelig kun å sørge for at det er samsvar mellom det angitte kontonummeret og den *faktiske* betalingsmottakeren.[26] 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

---

[20] Se eksempelvis «Avtalevilkår for BankAxept/Visa/Mastercard betalingskort og andre kortbaserte betalingsinstrumenter (debet) – forbruker» fra DNB punkt 6 om bruk av betalingskort.

[21] Prop. 92 LS (2019–2020) s. 276, jf. s. 279.

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

[23] En nærmere gjennomgang av dette faller utenfor artikkelens tema. Se nærmere i Line Utne Norland og Marte Eidsand Kjørven, «Elektoniske signaturer og avtalebidning», i Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad, red., *Bruk og misbruk av elektronisk identifikasjon*.

[24] Tilsvarende Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked artikkel 89.

[25] Tilsvarende Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked artikkel 88.

[26] Marte Eidsand Kjørven, «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. 91.

for å ha blitt lurt av en tredjeperson.[27] Ansvarsbegrensningene i § 4-30 kommer da ikke anvendelse.[28] Hvorvidt det i et konkret tilfelle foreligger et slik samtykke, kan imidlertid være uklart, og det kan oppstå flere grensetilfeller. I lys av artikkelens tema behandles imidlertid ikke dette nærmere her.

Hovedregelen om bankens ansvar for tap som skyldes ikke godkjente betalingstransaksjoner, innebærer en gjennomføring av PSD 2 artikkel 73. Det følger videre av artikkel 74 nr. 1 at kunden på sin side skal bære tap som skyldes «manglende opfyldelse af en eller flere af de forpligtelser, der er fastsat i artikel 69, begået med forsæt eller ved grov forsømmelse». I fjerde avsnitt fremgår det imidlertid at medlemsstatene kan velge å begrense kundens ansvar dersom kunden ikke har opptrådt svikaktig eller begått et forsettlig pliktbrudd. Lovgiver har for norsk retts vedkommende valgt å benytte seg av denne muligheten, idet ansvaret ved grov uaktsomhet er begrenset til 12 000 kroner når tapet er skjedd ved bruk av et «elektronisk betalingsinstrument», jf. finansavtaleloven (2020) § 4-30 tredje ledd.

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. finansavtaleloven (2020) § 1-5 annet ledd.[29] Med «betalingsoppdrag» menes «en anmodning fra en betaler eller betalingsmottaker til en betalingstjenesteyter om å foreta en betalingstransaksjon», jf. § 1-5 femte ledd. At betalingsinstrumentet er «elektronisk», innebærer at det er brukt et betalingsinstrument for gjennomføring av et betalingsoppdrag hvor dataene innsamles elektronisk – uten manuell kontroll av betalingen.[30]

Både forarbeidene til finansavtaleloven (2020) og finansavtaleloven (1999) forutsetter at bruk av betalingskort med tilhørende kode er omfattet av definisjonene, og det er på det rene at bruk av betalingskort til å gjennomføre en betalingstransaksjon utgjør bruk av et «elektronisk betalingsinstrument», jf. § 1-5 annet ledd.[31] Når BankID brukes som elektronisk autentisering til å iverksette betalingssansaksjoner i nettbanken, vil de prosedyrene som må følges, samlet utgjøre bruk av et betalingsinstrument.[32] Dette

---

[27] Marte Eidsand Kjørven, «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. 90.

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

[29] Tilsvarende Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked artikkel 4 nr. 14.

[30] Ot.prp. nr. 94 (2008–2009) s. 118 og Ot.prp. nr. 41 (1998–99) s. 43.

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

[32] Prop. 92 LS (2019–2020) s. 175.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

legges til grunn av Høyesterett i både HR-2020-2021-A avsnitt 38 og HR-2022-1752-A avsnitt 29.

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 finansavtaleloven (2020) § 4-30 jf. § 4-32 første ledd.

Reglene om ikke godkjente betalingstransaksjoner i § 4-30 gjelder i utgangspunktet både for kunder som er forbrukere, og kunder som er næringsdrivende, men er ufravikelige for forbrukere, jf. finansavtaleloven (2020) § 1-9. Artikkelen konsentrerer seg først og fremst om kunder som er forbrukere.

3 Kundens plikter

3.1 Innledende om kundens plikter og kundens varslingsplikt

Det følger av finansavtaleloven (2020) § 4-30 tredje ledd at ved misbruk av elektroniske betalingsinstrumenter er kunden ansvarlig for en egenandel på 12 000 kroner dersom «tapet skyldes at kunden ved grov uaktsomhet har unnlatt å oppfylle en eller flere av sine plikter etter § 4-23 første ledd eller § 4-24 første ledd». Vurderingen av kundens ansvar ved misbruk av elektroniske betalingsinstrumenter skjer altså i to steg: Det må først konstateres at det foreligger et pliktbrudd. Dernest må graden av skyld vurderes, ettersom dette er den avgjørende rettsvirkningen av pliktbruddet.[33]

Varslingsplikten i finansavtaleloven (2020) § 4-24 er en delvis videreføring av finansavtaleloven (1999) § 37 første ledd og § 40 fjerde ledd og gjennomfører PSD 2 artikkel 71. Bestemmelsen slår fast at kunden uten ugrunnet opphold skal varsle betalingstjenesteyteren, i tråd med opplysningene betalingstjenesteyteren har gitt i henhold til § 4-23 annet ledd, dersom kunden blir «oppmerksom på» tap, tyveri eller uberettiget bruk eller tilegnelse av et betalingsinstrument eller en konto. Med dette forstås at kunden må ha faktisk kunnskap om den ikke godkjente betalingstransaksjonen.[34] Dette innebærer at det ikke er tilstrekkelig at kunden burde ha blitt kjent med forholdet – slik det følger av ordlyden i finansavtaleloven (1999) § 37.

I tillegg til varslingsplikten i § 4-24 er kunden pålagt plikter ved utstedelse og bruk av betalingsinstrumentet etter § 4-23. Før jeg går nærmere inn på grensen for grov uaktsomhet, vil jeg i punkt 3.2 knytte noen kommentarer til innholdet av kundens forpliktelser etter § 4-23.

---

[33] Se HR-2022-1752-A avsnitt 37, hvor Høyesterett beskriver tilsvarende fremgangsmåte for finansavtaleloven (1999) § 35 tredje ledd.

[34] Prop. 92 LS (2019–2020) s. 380.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

3.2 Kundens plikter ved utstedelse og bruk av betalingsinstrument

Bestemmelsen i finansavtaleloven (2020) § 4-23 tilsvarer finansavtaleloven (1999) § 34 og gjennomfører PSD 2 artikkel 69 og deler av artikkel 70. Kunden pålegges etter denne bestemmelsen å bruke betalingsinstrumentet i samsvar med «vilkårene for utstedelse og bruk». Det er særskilt presisert at kunden 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.[35] Dette omfatter eksempelvis PIN-kode eller annet passord for å bekrefte iverksettelsen av en betalingstransaksjon, herunder kodebrikke og passord knyttet til en BankID.[36]

Hva som nærmere ligger i direktivets henvisning til at sikkerhetsinformasjonen skal være «personlig», er ikke definert verken i loven eller i direktivet. I forarbeidene til finansavtaleloven (1999) antas det at «personlig sikkerhetsinformasjon» henviser til at sikkerhetsinformasjonen etter avtalen med betalingstjenesteyter ikke skal oppgis til uvedkommende.[37] Dette betyr imidlertid ikke at informasjonen er personavhengig, slik som egen underskrift eller fødselsnummer, ettersom slik informasjon ikke er noe tjenesteyter har stilt til rådighet for kunden.

Som forklart ovenfor i punkt 2 følger kundens plikter nærmere av utstedelsesavtalene for betalingskort eller for BankID. Av disse avtalene følger det, med noe varierende ordlyd, at kunden skal ta alle rimelige forholdsregler for å beskytte kode og passord og ikke bruke betalingsinstrumentet slik at andre kan se koden eller passordet. Samtidig slås det fast at kode og passord ikke skal gjøres tilgjengelig for noen, heller ikke politiet eller banken.[38] Det er imidlertid høyst tvilsomt om en slik regulering i utstedelsesavtalen står seg, ettersom det blant annet ikke er mulig å kontraktsregulere hvilke opplysninger man plikter å gi til politiet.[39]

Betalingstjenesteyteren står ikke helt 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 siste punktum presiseres det at «[v]ilkårene for utstedelse og bruk skal være objektive, ikke innebære forskjellsbehandling og stå i forhold til formålet». Dette

---

[35] Tilsvarende Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked artikkel 4 nr. 31.

[36] Prop. 92 LS (2019–2020) s. 167 og HR-2022-1752-A avsnitt 30.

[37] Ot.prp. nr. 94 (2008–2009) s. 121 med videre henvisning til svenske forarbeider.

[38] Se DNB. «Avtalevilkår for BankAxept/Visa/Mastercard betalingskort og andre kortbaserte betalingsinstrumenter (debet) – forbruker». 2023. (hentet 31. mars 2023), punkt 5 og DNB. «Avtale om BankID». (u.å). (hentet 31. mars 2023), punkt 4.1.

[39] Se Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 338.

begrenser betalingstjenesteyters mulighet til å avtale seg ut av et eventuelt ansvar, uten at PSD 2 eller forarbeidene til finansavtaleloven (2020) konkretiserer dette nærmere.[40]

I tillegg stiller forbrukeravtaledirektivet, rådsdirektiv 93/13/EØF om urimelige vilkår i forbrukeravtale, krav til avtalens utforming og balanse i forbrukerforhold. Artikkel 5 første punktum slår fast at avtalevilkårene skal formuleres på en «klar og forståelig måte». EU-domstolen har slått fast at det i dette ligger mer enn at avtalens innhold skal være grammatisk riktig utformet.[41] 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.[42] For det andre pålegges næringsdrivende en forklaringsplikt, hvor forbrukeren må opplyses om avtalevilkårene og konsekvensene av disse før avtalen inngås.[43] Dette supplerer betalingstjenesteyters opplysningsplikt etter finansavtaleloven (2020) § 3-31 og vil være en sentral tolkningsfaktor ved tolkningen av utstedelsesavtalen.

Loven pålegger kunden å ta «alle rimelige forholdsregler» for å beskytte «personlig sikkerhetsinformasjon», jf. § 4-23. 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 Høyesterett seg i avsnitt 98 om hva som ligger i «rimelige forholdsregler» etter finansavtaleloven (1999) § 34:

«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.[44]

Hva som utgjør rimelige forholdsregler, må vurderes med utgangspunkt i hvordan betalingsinstrumentet brukes og oppbevares. Det er av den grunn nærliggende å lese kravet om at kunden skal ta alle «rimelige forholdsregler» for å beskytte sin personlige sikkerhetsinformasjon, i sammenheng med kravet om at betalingsinstrumentet skal brukes «i samsvar med vilkårene for utstedelse og bruk». Eksempelvis har ikke kunden tatt alle rimelige forholdsregler dersom et betalingsinstrument oppbevares nedlåst i en koffert sammen med tilhørende kode eller passord nedskrevet på et ark.[45] Kunden

---

[40] Se nærmere om kundens plikt til å beskytte sikkerhetsinformasjon i Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 337 flg.

[41] Sak C-26/13 *Kásler og Rábai mot OTP Jelzálogbank Zrt.* avsnitt 71.

[42] Sak C-26/13 *Kásler og Rábai mot OTP Jelzálogbank Zrt.* avsnitt 74.

[43] Sak C-186/16 *Andriciuc mfl. mot Banca Românească SA* avsnitt 47.

[44] Børge Grøttjord og Karl Rosén, *Finansavtaleloven: med kommentarer*, Gyldendal, 2014, s. 205.

[45] Slik som i Rt-2004-499, se nærmere i punkt 7.2.

holdes imidlertid ikke ansvarlig for ethvert avvik fra disse pliktene. Det kreves at kunden har utvist grov uaktsomhet eller forsett for at kunden skal holdes ansvarlig utover egenandelen på 450 kroner, jf. § 4-30 annet ledd.

4 Vurderingstemaet for grovt uaktsomt pliktbrudd

Som forklart i innledningen er systemet i finansavtaleloven at betalingstjenesteyterens ansvar blir redusert i tråd med graden av klander fra kunden.[46] Verken finansavtaleloven (1999) eller finansavtaleloven (2020) definerer uttrykket «grov uaktsomhet». Ordlyden tilsier at det er tale om en høy terskel, slik at bestemmelsen er reservert for de mer alvorlige tilfellene av pliktforsømmelser, begrenset oppad mot forsett.

Heller ikke i PSD 2 er begrepet definert, men fortalen gir enkelte anvisninger om terskelen. I punkt 72 i fortalen fremgår 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 …».

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.

Videre følger det av fortalen punkt 72 at «[b]eviset for og graden af den påståede forsømmelse bør generelt vurderes i henhold til national ret». Denne henvisningen til nasjonal rett er noe underlig, ettersom PSD 2 i utgangspunktet er et fullharmoniseringsdirektiv, se artikkel 107. Fullharmonisering kan nødvendigvis ikke oppnås dersom man skal bygge på ulike nasjonale konsepter av grov uaktsomhet.[47] I alle tilfelle må fortalens henvisning til nasjonal rett på dette punktet, sammenholdt med fraværet av nærmere retningslinjer i PSD 2 selv eller andre EØS-rettslige kilder, innebære at det er adgang til å trekke inn nasjonale kilder i rettsanvendelsen.

I forarbeidene til finansavtaleloven (1999) uttales det i denne forbindelse at «[f]or at kunden skal anses å ha vært grovt uaktsom, kreves det … et markert avvik fra vanlig

---

[46] Se HR-2022-1752-A avsnitt 35–37.

[47] Se nærmere om dette i Marte Eidsand Kjørven, «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 med videre henvisninger. Se også Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 341 flg. om skyldvurderingen etter PSD 2.

forsvarlig handlemåte».[48] Denne formuleringen av vurderingstema tilsvarer det som fremgår av fortalen til PSD 2, og samsvarer med utgangspunktet i norsk kontraktsrett.[49] Høyesterett bygger videre på dette utgangspunktet i Rt-2004-499, som til nå er den eneste saken hvor Høyesterett har vurdert terskelen for grovt uaktsomme pliktbrudd ved ikke godkjente betalingstransaksjoner.

Høyesterett slår i avsnitt 32 fast at kunden må ha utvist en kvalifisert form for uaktsomhet. Kundens handlinger må representere «et markert avvik fra vanlig forsvarlig handlemåte», og 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». Dette tilfører imidlertid ikke noe mer enn det som allerede følger av PSD 2 og uttalelsen i forarbeidene til finansavtaleloven (1999). Dommen kommenteres nærmere under punkt 7.2. Med disse generelle utgangspunktene som grunnlag skal jeg nå gå nærmere inn på hvorvidt (a) kundens individuelle forhold og (b) manglende sikkerhetsrutiner hos betalingstjenesteyteren er relevant å vektlegge i vurderingen av om kunden har opptrådt grovt uaktsomt. Dette behandles videre i henholdsvis punkt 5 og punkt 6.

5 Betydningen av kundens individuelle forhold

Aktsomhetsvurderingen etter finansavtaleloven (2020) § 4-30 er knyttet til hvorvidt «kunden» har handlet grovt uaktsomt. Spørsmålet i dette punktet er hvorvidt kundens individuelle forhold kan ha innvirkning på aktsomhetsvurderingen, eller om kunden måles etter en rent objektiv målestokk, basert på gjennomsnittsforbrukeren. Om kunden lar seg lure av ulike svindelmetoder, vil i mange tilfeller bero på personlige forutsetninger, og det er derfor relevant å vurdere hvorvidt dette skal vektlegges i aktsomhetsvurderingen etter § 4-30.

Ordlyden i § 4-30 berører ikke kundens individuelle forhold eller personlige forutsetninger for å kunne avdekke svindel. Heller ikke PSD 2 går nærmere inn på temaet. I forarbeidene til finansavtaleloven (2020) forutsettes det imidlertid i tilknytning til vurderingen av forsettlige pliktbrudd at «eldre personer … som har behov for hjelp av andre til å betale regninger» ikke skal være ansvarlige for hele det økonomiske tapet.[50]

Videre samme sted følger det at kunder som har behov for hjelp på grunn av mangelfulle språkkunnskaper, ikke uten videre kan holdes ansvarlige for forsettlige pliktbrudd. Med

---

[48] Se Ot.prp. nr. 94 (2008–2009) s. 117.

[49] Se Viggo Hagstrøm mfl., *Obligasjonsrett,* 3. utg. ved Herman Bruserud mfl., Universitetsforlaget, 2021, s. 507, hvor det fremheves at grov uaktsomhet først foreligger når kontraktspartens opptreden er kvalifisert klanderverdig og foranlediger sterke bebreidelser for mangel på aktsomhet.

[50] Innst. 104 L (2020–2021) s. 22. Uttalelsene gjelder reglene om misbruk av elektronisk signatur, jf. § 3-20, men lovgiver har forutsatt lik forståelse av reglene om henholdsvis misbruk av elektronisk signatur og ikke godkjente betalingstransaksjoner. Merk ellers at det som er mindretallets uttalelser i komiteen, er det som senere ble vedtatt med flertall på Stortinget.

dette legger forarbeidene til grunn at også manglende språkkunnskaper er et relevant individuelt forhold i 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».[51]

Forarbeidene trekker med dette frem at kundens høye alder eller mangelfulle språkkunnskap etter omstendighetene kan være relevante momenter i skyldvurderingen. Med dette åpner lovgiver for at skyldvurderingen etter § 4-30 kan påvirkes av individuelle forhold hos kunden. Selv om kun disse forholdene er nevnt, kan forarbeidene neppe forstås slik at det ikke er aktuelt å legge vekt på andre individuelle forhold hos kunden.

Individuelle forhold trekkes frem som relevante momenter i både erstatningsretten og kontraktsretten.[52] I erstatningsretten kan subjektive forhold være avgjørende for aktsomhetsvurderingen, der det eksempelvis stilles lempeligere krav til barn enn til voksne.[53] Innenfor erstatningsrettslig teori hevdes det også at høy alder i kombinasjon med alderdomssvekkelser kan føre til en mildere aktsomhetsbedømmelse.[54]

Samtidig taler reelle hensyn for at slike individuelle forhold er relevant å vektlegge, ettersom det er liten tvil om at slike forhold påvirker kundens mulighet til å avdekke svindel. Særlig fremheves det at det har oppstått et kunnskapsgap mellom yngre og eldre generasjoner med hensyn til teknologi og bruk av digitale løsninger som følge av den digitale utviklingen. Dette medfører at en avgrenset gruppe mennesker er særlig utsatt for svindel. 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 egen hånd. Disse kundene søker gjerne hjelp hos familie og venner, som innebærer at risikoen for svindel øker.[55] Svindlere utnytter denne mangelen på digital kunnskap, som særlig vises gjennom sakene om såkalt Olga-svindel, hvor svindlere målrettet kontakter eldre mennesker. Individuelle forhold hos kunden kan – og bør – følgelig være et viktig moment i aktsomhetsvurderingen ved misbruk av elektroniske betalingsinstrumenter.

Når det gjelder språkkunnskap, har problemstillingen tidligere blitt behandlet av lagmannsretten i LB-2016-43622 etter finansavtaleloven (1999). Saken gjaldt en kvinne som på grunn av begrensede norskkunnskaper overlot BankID og passord til sin

---

[51] NOU 2008: 21 s. 105.

[52] Viggo Hagstrøm mfl., *Obligasjonsrett,* 3. utg. ved Herman Bruserud mfl., Universitetsforlaget, 2021 og Viggo Hagstrøm og Are Stenvik, *Erstatningsrett,* 2. utg., Universitetsforlaget, 2019, s. 169.

[53] Viggo Hagstrøm og Are Stenvik, *Erstatningsrett,* 2. utg., Universitetsforlaget, 2019, s. 171.

[54] Viggo Hagstrøm og Are Stenvik, *Erstatningsrett,* 2. utg., Universitetsforlaget, 2019, s. 172.

[55] Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2020.* Finanstilsynet, 2020. (hentet 25. juli 2022), s. 42.

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, slik at finansavtaleloven (1999)s bestemmelser om tapsbegrensning ved uautoriserte betalingstransaksjoner i § 35 ikke kom til anvendelse. Alminnelig erstatningsrett var altså det rettslige grunnlaget for kundens ansvar. 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 språkkunnskaper ble ikke tillagt vekt, og lagmannsretten anså det som uaktsomt av kunden å undertegne en avtale uten å sette seg inn i hva hun forpliktet seg til.

Dette vil imidlertid harmonere dårlig med betalingstjenesteyterens opplysnings- og forklaringsplikt, som ble berørt ovenfor i punkt 3.2. 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 tilstrekkelige språkkunnskaper til selv å sette seg inn i dette.

Til sammenlikning har Högsta domstolen i Sverige i en avgjørelse fra 21. juni 2022 uttrykkelig fremhevet individuelle forhold hos kunden ved aktsomhetsvurderingen.[56] Saken er relevant å fremheve, ettersom reglene om tapsfordeling ved misbruk av elektroniske betalingsinstrumenter i svensk rett, i likhet med i norsk rett, bygger på PSD 2. Den aktuelle saken gjaldt et tilfelle der en kunde ble fralurt personlig sikkerhetsinformasjon tilknyttet sin BankID som gjorde det mulig for svindlerne å overføre 397 000 svenske kroner fra kundens konto. Spørsmålet for retten var om kunden hadde handlet særskilt klanderverdig («särskilt klandervärt»). Domstolen kom til at dette ikke var tilfellet, og konkluderte med at kunden hadde handlet grovt uaktsomt («grovt vårdslöst»).[57] Kundens ansvar ble begrenset til 12 000 kroner. Ved skyldvurderingen uttales det i avsnitt 28:

«Vid bedömningen av ett eventuellt ansvar när konsumenten i samband med ett bedrägeri inte har skyddat sina personliga behörighetsfunktioner knutna till betalnings instrumentet finns det anledning att fästa särskilt avseende vid vissa faktorer. Bland dessa ingår den miljö och situation som konsumenten befann sig i samt hans eller hennes möjlighet att skydda sig mot en obehörig transaktion. Konsumentens ålder och erfarenhet kan här vara av betydelse ....» (Min utheving.)

Selv om utgangspunktet for aktsomhetsvurderingen er objektivt, peker Högsta domstolen uttrykkelig på at individuelle faktorer er sentrale ved aktsomhetsvurderingen,

[56] Högsta domstolen, dom av 21. juni 2022, mål T 4623-21.

[57] I Sverige graderes kundens skyld ut fra om vedkommende har handlet grovt uaktsomt («grovt vårdslöst»), der kundens ansvar er begrenset til 12 000 kroner, eller særskilt klanderverdig («särskilt klandervärt»), der kundens ansvar er ubegrenset. Har ikke kunden handlet grovt uaktsomt eller særskilt klanderverdig, er ansvaret begrenset til en egenandel på 400 kroner.

herunder miljøet og situasjonen kunden befinner seg i, kundens handlingsalternativer og kundens erfaring og alder. Gode grunner taler derfor for at aktsomhetsvurderingen må tilpasses kundens individuelle forutsetninger, tilsvarende slik Högsta domstolen gjør. Forarbeidene til finansavtaleloven (2020) åpner for at subjektive forhold etter omstendighetene kan være relevant ved skyldvurderingen, og trekker frem alder og språkkunnskap som eksempler på subjektive forhold. Det vil bære galt av sted dersom alle kunder vurderes etter samme objektive norm – det er med andre ord rom for individuelle tilpasninger basert på de konkrete omstendighetene. Samtidig må det understrekes at kunden ikke bevisst kan holde seg selv i villfarelse om hvilke forpliktelser vedkommende har, og på den måten omgå ansvarsreglene i finansavtaleloven.[58]

6 Betydningen av manglende sikkerhetsrutiner hos betalingstjenesteyteren

I forlengelsen av punktet ovenfor er det også relevant å spørre om forhold hos betalingstjenesteyteren kan påvirke vurderingen av hvorvidt kunden har handlet grovt uaktsomt. Særlig relevant er dette i de tilfellene der betalingstjenesteyteren, eksempelvis en bank, ikke har overholdt de sikkerhets- og kontrollrutiner den er pålagt.

Denne problematikken ble i korthet belyst av Høyesterett i HR-2020-2021-A. Saken gjaldt misbruk av elektronisk signatur før ikrafttredelsen av finansavtaleloven (2020), hvor slike tilfeller falt utenfor ansvarsbegrensningene i finansavtaleloven (1999). I avsnitt 50 flg. redegjør Høyesterett for ansvarsgrunnlaget for erstatning etter alminnelige erstatningsrettslige regler. Retten fremhever at rolleforventningen hos skadelidte og skadelidtes forhold i enkelte situasjoner kan medføre at skadelidte selv har den objektive egenrisikoen for skaden.[59]

Når BankID brukes utenfor det Høyesterett betegner som det opprinnelige bruksområdet – betalingstransaksjoner –, kan situasjonen være slik at det forventes at banken treffer sikkerhets- og kontrolltiltak utover å konstatere at BankID er riktig brukt.[60] I et *obiter dictum* legger imidlertid Høyesterett til grunn motsatt standpunkt ved ikke godkjente betalingstransaksjoner:[61]

---

[58] Et sentralt poeng her er at villfarelse om rettslige eller faktiske omstendigheter ikke alene kan begrunne at kunden har opptrådt grovt uaktsomt, ettersom dette er selvstendige ansvarsgrunnlag og ikke utmålingsregler. Spørsmålet aktualiseres særlig i de tilfellene der banken påstår at det foreligger et forsettlig pliktbrudd. Se nærmere om dette i Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 351 flg.

[59] HR-2020-2021-A avsnitt 57.

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

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

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

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

Høyesterett legger altså til grunn at det er tilstrekkelig for betalingstjenesteyteren å godtgjøre at BankID er brukt riktig ved gjennomføring av betalingstransaksjoner. Hvis det er tilfellet, vil skyldvurderingen i så fall bero på en isolert vurdering av hva *kunden selv* kunne og burde ha gjort.

Ettersom uttalelsen er knyttet til skyldreglene i 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). I denne sammenheng følger det av delegert kommisjonsforordning (EU) 2018/389 artikkel 2 nr. 1, som utfyller PSD 2, at betalingstjenesteytere plikter å ha «transaktionsovervågningsmekanismer, som sætter dem i stand til at afsløre uautoriserede eller svigagtige betalingstransaktioner».[62] Med andre ord plikter betalingstjenesteytere å ha sikkerhets- og kontrollrutiner på plass når BankID, eller for den saks skyld ethvert annet elektronisk betalingsinstrument, benyttes for gjennomføring av betalingstransaksjoner. At dette ikke løftes frem av Høyesterett, skyldes nok at saken ikke gjaldt betalingstransaksjoner, og at det av denne grunn ikke var behov for å behandle dette i dybden.

Betalingstjenesteyteren skal altså ha rutiner på plass for å overvåke betalingstransaksjoner med det formål å avdekke svindel og misbruk av betalingsinstrumenter. Den samme delegerte kommisjonsforordningen definerer i artikkel 18 nr. 2 bokstav c en rekke risikokriterier som betalingstjenesteyter skal vurdere ved transaksjonsovervåkningen, nemlig (i) «unormale udgifts- eller adfærdsmønstre hos betaleren», (ii) «usædvanlige oplysninger om betalerens adgang til anordninger og software», (iii) «malware-infektion i autentifikationsprocedurens sessioner», (iv) «kendte scenarier for svig i forbindelse med udbud af betalingstjenester», (v) «unormalt opholdssted for betaleren» og (vi) «højrisikoopholdssted for betalingsmodtageren».

På denne bakgrunn kan det spørres om mangel på sikkerhets- og kontrolltiltak hos betalingstjenesteyter som kunne avdekket og helt eller delvis hindret gjennomføringen av ikke-godkjente betalingstransaksjoner, må vektlegges ved vurderingen av om kunden har handlet grovt uaktsomt.

---

[62] Kommisjonsforordningen er med virkning fra 1. mai 2022 inkorporert i EØS-avtalen, se EØS-komiteens beslutning nr. 159/2020 av 23. oktober 2020 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester).

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Bestemmelsene om tapsfordeling i PSD 2 artikkel 74 og finansavtaleloven (2020) § 4-30 er utelukkende knyttet til de handlinger kunden selv foretar seg, og tar ikke opp de plikter betalingstjenesteyteren har og må følge. Direktivet går ikke nærmere inn på dette, og problematikken er heller ikke behandlet i forarbeidene til finansavtaleloven (2020) for betalingstransaksjoners vedkommende. Dette innebærer at det er uklart hvilken betydning forhold hos betalingstjenesteyteren har for vurderingen av kundens skyld i disse tilfellene.

I HR-2020-2021-A ble skadelidtes forhold uttrykkelig fremhevet. Saken gjaldt riktignok misbruk av elektronisk signatur, hvor Høyesterett langt på vei begrunnet at kunden ikke hadde handlet uaktsomt, med henvisning til skadelidtes (bankens) forhold.[63] Merk at Høyesterett her la til grunn at det ikke kreves ytterligere kontroll- og sikkerhetstiltak der BankID er riktig brukt ved gjennomføring av betalingstransaksjoner, men som vist ovenfor er nok ikke dette helt treffende.

I fravær av nærmere begrunnelse er ikke Høyesteretts standpunkt særlig overbevisende. I lys av det ovennevnte, og at det er tale om et *obiter dictum*, er det derfor tvilsomt om fremtidige avgjørelser bør legge til grunn det samme standpunktet. Hvis betalingstjenesteyter ikke overholder sin plikt til å overvåke mistenkelige betalingstransaksjoner, som kunne satt dem i stand til å hindre eller begrense tap som følge av en ikke-godkjent betalingstransaksjon, taler gode grunner for at dette kan spille inn i vurderingen av kundens skyld, enten BankID er brukt til å gjennomføre betalingstransaksjoner eller til lånopptak. Dette vil være i tråd med erstatnings- og kontraktsrettslige synspunkter om at skadelidtes forhold kan ha betydning for den normative avveiningen av hvem som er nærmest til å bære risikoen.[64] Manglende etterfølgelse av pålagte kontroll- og sikkerhetstiltak innebærer at betalingstjenesteyteren bevisst eksponerer seg selv for en risiko.

Tilsvarende synspunkter har blitt reist under andre jurisdiksjoner i EU. Særlig er det verdt å fremheve at Portugals høyesterett ved flere anledninger har konkludert at betalingstjenesteyter burde ha oppdaget at det var tale om ikke godkjente betalingstransaksjoner på bakgrunn av at transaksjonene som ble gjennomført, avvek fra kundens normale handlemønstre.[65] Tilsvarende som ovenfor argumenteres det for at betalingstjenesteyters forpliktelser etter delegert kommisjonsforordning (EU) 2018/389,

---

[63] HR-2020-2012-A avsnitt 104.

[64] Morten Kjelland, *Erstatningsrett. En lærebok,* 2. utg., Universitetsforlaget, 2019, s. 97–98 og Viggo Hagstrøm mfl., *Obligasjonsrett,* 3. utg. ved Herman Bruserud mfl., Universitetsforlaget, 2021, s. 617.

[65] Maria Raquel Guimarães og Reinhard Steennot, «Allocation of liability in case of payment fraud: Who bears the risk of innovation: A comparison of Belgian and Portuguese law in the context of PSD2», *European Review of Private Law,* årg. 30, nr. 1, 2022, s. 69–70.

og manglende etterfølgelse av de kontroll- og sikkerhetstiltak som pålegges betalingstjenesteyteren, må ha betydning for vurderingen av kundens skyld.[66]

Basert på dette kan det med god grunn argumenteres for at betalingstjenesteyter plikter å ha kontroll- og sikkerhetstiltak som gjør det mulig å identifisere ikke godkjente betalingstransaksjoner. Det er ikke nødvendigvis slik at det er tilstrekkelig at betalingstjenesteyter godtgjør at det enkelte elektroniske betalingsinstrument, det være seg BankID eller betalingskort, er brukt på riktig måte; manglende kontroll- og sikkerhetstiltak bør ha betydning i vurderingen av kundens skyld. Under enhver omstendighet er dette forhold som er relevant å vektlegge ved en eventuell vurdering av om kundens ansvar skal lempes etter finansavtaleloven (2020) § 4-31. Det faller imidlertid utenfor temaet for denne artikkelen å gå nærmere inn på spørsmål om lemping.

7 Grov uaktsomhet i utvalgte typetilfeller av ikke godkjente betalingstransaksjoner

7.1 Innledende om typetilfellene

Praksis fra Finansklagenemnda viser at spørsmål om hvorvidt kunden har opptrådt grovt uaktsomt, typisk oppstår enten (1) fordi en tredjeperson har fått tilgang til sikkerhetsinformasjon fordi denne var nedtegnet, (2) fordi kunden er utsatt for skriftlig *phishing* via e-post eller sms, eller (3) fordi kunden er utsatt for *vishing* (telefonsvindel). Det er derfor av særlig interesse å vurdere disse tre typetilfellene opp mot terskelen for grov uaktsomhet, som vil bli behandlet i de neste punktene.

7.2 Kan det være grovt uaktsomt å skrive ned personlig sikkerhetsinformasjon som PIN-kode og passord?

I dette punktet er spørsmålet om det kan være grovt uaktsomt å skrive ned personlig sikkerhetsinformasjon. Med andre ord er vurderingen om det er en «rimelig forholdsregel» for å beskytte denne sikkerhetsinformasjonen at PIN-kode og passord ikke skrives ned. Utstedelsesavtalene for BankID og betalingskort forbyr ikke å skrive ned personlig sikkerhetsinformasjon, slik som PIN-kode tilknyttet betalingskort eller passord knyttet til BankID. På grunn av mengden koder og passord man må ha kontroll på, er det mange som tyr til å skrive ned disse for å få bedre kontroll og oversikt. Nedtegningen kan skje enten fysisk på papir eller digitalt på eksempelvis telefonen.

At nedtegning av PIN-kode og passord medfører økt risiko for misbruk, er åpenbart, og det anbefales at man heller har gode og unike passord som skrives ned og oppbevares

[66] Maria Raquel Guimarães og Reinhard Steennot, «Allocation of liability in case of payment fraud: Who bears the risk of innovation: A comparison of Belgian and Portuguese law in the context of PSD2», *European Review of Private Law,* årg. 30, nr. 1, 2022, s. 71–72.

trygt, enn å ha enkle passord eller samme passord som brukes over flere tjenester.[67] Samtidig følger det av fortalen til PSD 2 punkt 72 at «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» utgjør et grovt uaktsom pliktbrudd. Hvordan den nedskrevne koden eller passordet og betalingsinstrumentet oppbevares, er altså sentralt for vurderingen av grov uaktsomhet.

Høyesterett har bare ved ett tilfelle behandlet spørsmålet om grovt uaktsomme pliktbrudd ved misbruk av elektroniske betalingsinstrumenter, nemlig i Rt-2004-499. Ettersom dette er den eneste avgjørelsen fra Høyesterett som tar stilling til kundens aktsomhet ved ikke godkjente betalingstransaksjoner, vil de generelle merknadene rundt terskelen for grov uaktsomhet fortsatt være retningsgivende til tross for dommens alder. Utgangspunktene har også blitt gjentatt i nyere underrettspraksis.[68]

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 som kortene. Høyesterett delte seg tre mot to, hvor flertallet konkluderte med at kunden ikke hadde opptrådt grovt uaktsomt.

Ved tolkningen av uttrykket «grov uaktsomhet» slo flertallet fast at kunden må ha utvist en kvalifisert form for uaktsomhet.[69] Som nevnt under punkt 4 må en grovt uaktsom oppførsel representere «et markert avvik fra vanlig forsvarlig handlemåte», og 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». Dette innebærer at det for det første må foreligge et objektivt avvik fra en vanlig forsvarlig handlenorm.

Det følger av flertallets videre drøftelse at utgangspunktet for vurderingen er den «alminnelige kortholder». Standarden er med andre ord ikke hvordan idealkunden ville handlet. Dette objektive avviket må være «markert», som innebærer at ikke ethvert avvik fra den alminnelige handlenormen vil omfattes. 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» enn ved alminnelig uaktsomhet. Her er det rom for å tillegge individuelle forhold ved kunden vekt, se nærmere under punkt 5.

---

[67] NorSIS. *Trusler og trender 2021*. NorSIS, 2021. https://norsis.no/publikasjoner/ (hentet 4. november 2022), s. 12–13.

[68] Se eksempelvis TOSLO-2018-180834, TFRED-2019-63291 og TSOFT-2017-175325 (hvorav de to sistnevnte gjaldt misbruk av elektronisk signatur).

[69] Rt-2004-499 avsnitt 32.

I den konkrete vurderingen var det sentralt om koden var notert slik at det muliggjorde en tredjepersons misbruk av kortet. Flertallet slo fast at «folk flest» antakelig ville hatt vanskeligheter med å finne riktig kode. Høyesterett trakk frem to sentrale forhold i vurderingen av om uaktsomheten kunne kategoriseres som grov, nemlig at koden kunne vært kamuflert bedre, og at kunden kunne redusert risikoen for svindel betydelig ved å ta med seg notatboken. Det sentrale i skyldvurderingen er altså kundens handlingsalternativer, hvor det var «ubetenksomt» å la kort og kode ligge sammen, til tross for at de var nedlåst i en koffert i en forsvarlig låst leilighet som ikke var spesielt utsatt for innbrudd. 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.

Høyesteretts flertall 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». 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.

Avslutningsvis påpekte 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 som Høyesterett oppstiller, nemlig 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» (avsnitt 41). 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 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, ettersom det skaper en høyst uforutsigbar stilling i avtaleforholdet med betalingstjenesteyteren. 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 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.

Høyesteretts avgjørelse har i hovedsak blitt fulgt opp i liknende saker som har kommet opp for Finansklagenemnda. Praksisen viser at det gjennomgående slås fast at kunden har opptrådt grovt uaktsomt dersom koden har blitt oppbevart sammen med kortet i åpen eller dårlig kamuflert form.[70] Oppbevares koden *adskilt* fra betalingsinstrumentet, vil vurderingen bero på et samspill mellom 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 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.[71]

7.3 Kan det være grovt uaktsomt å falle for phishing-angrep?

I dette punktet er spørsmålet om det er grovt uaktsomt av kunden å falle for phishing-svindel. Med dette menes, som forklart innledningsvis, tilfeller der kunden blir lurt til å følge en digital lenke vedkommende har mottatt på e-post, sms eller liknende. Lenken dirigerer kunden til en side som i større eller mindre grad likner på nettsiden til kundens bank eller en annen aktør. Svindlerne har kontroll over narresiden og 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 det foreligger et objektivt pliktbrudd ved at kunden har delt personlig sikkerhetsinformasjon med uvedkommende i strid med utstedelsesavtalen.

Høyesteretts avgjørelse i Rt-2004-499 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 må være 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.

---

[70] Eksempelvis FinKN-2022-324, FinKN-2020-230, FinKN-2020-52 og FinKN-2017-580.

[71] Eksempelvis FinKN-2013-276, hvor nemnda konkluderte med at det ikke var grovt uaktsomt å oppbevare kort og kode i eget hjem, selv om koden var notert i klartekst.

Kontakten skjer 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 å 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 henvendelsen og til å tvile på om den er reell. Dernest kan språket være avslørende; dårlig språk vil være et tegn på at det ikke er kundens faktiske bank som tar kontakt. Kombinasjonen av disse elementene kan innebære at kunden har handlet grovt uaktsomt. Denne vurderingen vil påvirkes av kundens personlige forutsetninger, slik som språkkunnskap, jf. ovenfor i punkt 5. 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 står kundens handlingsalternativer sentralt. På den ene side kan kunden fullstendig avstå fra å trykke på slike lenker. Dette innebærer en risiko for å gå glipp av viktig informasjon som blir tilsendt kunden, og kan derfor ikke anses som et reelt alternativ. På den annen 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 med en lenke til en nettside hvor de ble bedt om å registrere seg med BankID dersom de ønsket vaksine mot covid-19.[72] 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, og Høyesterett har uttrykkelig slått fast at kunden «må ta hensyn til» at det finnes profesjonelle svindelmetoder.[73] Prinsippet som Høyesterett uttrykker, er relevant også ved phishing.

---

[72] Sofie Grønntun Nissen 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 28. februar 2022).

[73] Rt-2004-499 avsnitt 36.

Kjørven, Marte Eidsand, Hjort, Maria Astrup og Wærstad, Tone Linn (red.). *Bruk og misbruk av elektronisk identifikasjon*. 1. utg., Oslo: Karnov, 2025.

Det vil si at når visse svindelmetoder er et kjent fenomen, vil det etter omstendighetene kunne stilles strengere krav til kundens aktsomhet. Det kan imidlertid være vanskelig å skille de reelle henvendelsene fra svindelforsøkene, all den tid både offentlige og private aktører, herunder banker og diverse abonnementstjenester, faktisk sender slike meldinger til forbrukere.[74] Mens forbrukere på den ene side gjennom informasjonskampanjer frarådes å trykke på digitale lenker og oppgi BankID-passord, driver seriøse aktører på den annen 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.

Vurderingen av kundens aktsomhet beror altså på en samlet vurdering av en rekke elementer ved den enkelte henvendelse. Det er i dag ingen publiserte rettsavgjørelser som omhandler spørsmålet om skyld ved phishing ved ikke godkjente betalingstransaksjoner. Finansklagenemnda har imidlertid hatt en rekke slike saker til behandling, og i motsetning til betraktningene ovenfor har nemnda hovedsakelig ansett det som grovt uaktsomt å falle for phishing. Som jeg vil vise i fortsettelsen, har Finansklagenemnda frem til nylig lagt seg på en strengere linje enn betraktningene ovenfor om hva som utgjør grov uaktsomhet, uten at det kan sies at det foreligger rettslig grunnlag for dette.

En av de første sakene Finansklagenemnda behandlet som gjaldt spørsmålet om ansvarsfordeling etter phishing, gjaldt en forbruker som hadde mottatt en e-post som tilsynelatende så ut som den kom fra Apple:[75]

«Sakens dokumenter viser at både eposten og den nettsiden klageren ble ledet inn på, var troverdige. Adressen i lenken var, slik den kunne leses av kortholderen på skjermen, identisk med Apples korrekte internettadresse. Lenken førte likevel ikke dit, men til en falsk side. Nemnda forstår det slik at det var vanskelig eller umulig for kortholderen å se at siden ikke var ekte. Grov uaktsomhet må derfor i tilfelle begrunnes med at hun fulgte en lenke i en epost i stedet for selv aktivt å taste inn adressen. Nemnda mener at med den publisitet som finnes om svindel og med de advarsler som gis mot å la seg svindle på denne måten, må det regnes som grovt uaktsomt å gi kortopplysninger på denne måten, selv om både eposten og nettsiden var svært troverdig.»

Nemnda legger seg altså på en linje der det å falle for et phishing-angrep i seg selv regnes som grovt uaktsomt, selv i et tilfelle der det var «vanskelig eller umulig» for

---

[74] Marte Eidsand Kjørven, «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. 93 og Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2022.* Finanstilsynet, 2022. (hentet 25. juli 2022), s. 32.

[75] FinKN-2017-506.

kunden å avsløre at det dreide seg om svindel. Denne linjen ble fulgt opp i senere praksis.

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 en automatisk svarer hos (reelle) Netflix. Kunden fattet dermed ikke mistanke om svindel, sammenliknbart med eksemplet med Oslo kommune ovenfor. Nemnda la imidlertid 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». Nemndas begrunnelse for at pliktbruddet var grovt uaktsomt, er altså hovedsakelig forankret i at phishing er en kjent svindelmetode, samtidig som nemnda i vurderingen velger å se bort fra 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» hadde mulig sammenheng med at han hadde vært på handelsmesser tidligere samme dag, og at kontoen i denne forbindelse kunne ha blitt «hacket». 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 «allment kjent», noe som er en høyst usikker påstand fra Finansklagenemnda, ble dette ansett som grovt uaktsomt. Mindretallet påpekte imidlertid at e-posten var profesjonelt utformet, og at avsenderadressen var troverdig. Dette, sett i sammenheng 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.[76]

Sakene viser at Finansklagenemnda i mindre grad er villig til å legge vekt på konkrete forhold ved den enkelte henvendelsen som kan medføre at kunden ikke har grunn til å reagere, hvor den vektlegger at phishing er en kjent svindelmetode, og selve budskapet i

[76] Tilsvarende i FinKN-2022-54, som gjaldt et liknende forhold.

henvendelsen. Dette var også tilfellet i FinKN-2019-681, hvor kunden ifølge flertallet handlet grovt uaktsomt da 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 fremsto slik svindel som et utbredt og omfattende problem, og at «denne type kriminalitet ikke enkel 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 den 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.[77]

Nemndas begrunnelse i liknende saker bygger hovedsakelig på en kombinasjon av at den 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.[78] Som jeg vil komme tilbake til lenger ned, er disse avgjørelsene neppe uttrykk for gjeldende rett.

At phishing er en svindelmetode som mange personer faller for, ble tatt opp i FinKN-2018-46, men nemnda valgte å avvise saken fra nærmere behandling. Nemnda påpeker at den har erfart at BankID som innloggingsverktøy brukes av flere aktører enn forutsatt i tidligere saker, som etter nemndas syn gjør det mindre påfallende og mindre mistenkelig å bli anmodet om å logge inn med BankID. Videre påpekes det at dette kan skape inntrykk av at det er trygt å 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.[79]

I de tilfellene nemnda har konkludert med 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 og 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

[77] Tilsvarende i FinKN-2019-683.

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

[79] Finanstilsynet. *Risiko- og sårbarhetsanalyse (ROS) 2022*. Finanstilsynet, 2022. (hentet 25. juli 2022), s. 31.

såpass spesielle omstendigheter at kunden ikke kunne anses å ha handlet grovt uaktsomt.[80]

Disse sakene utgjør imidlertid unntaket fra Finansklagenemndas nokså strenge praksis. Nyere uttalelser fra 2021 og 2022 kan imidlertid tas til inntekt for at Finansklagenemnda er i ferd med å endre kurs og i større grad konkluderer med at kunden ikke har handlet grovt uaktsomt, noe FinKN-2021-788 er et eksempel på. Her hadde klageren mottatt en e-post som angivelig kom fra portalen *Jobbnorge*, med invitasjon til jobbintervju. For å bekrefte intervjuet måtte klageren følge en lenke og logge inn med BankID. Klageren fulgte lenken, med den følge at det ble gjennomført en transaksjon på 27 000 kroner. Nemnda vurderte at klageren ikke hadde handlet grovt uaktsomt, ettersom «saken skiller seg fra det som tidligere har vært vanlig i saker om phishing ved at svindleren har lyktes i å komme inn i en pågående prosess mellom klageren og den aktøren som den falske e-posten angivelig kommer fra».[81]

I FinKN-2021-1110 var tilfellet det at kunden ventet en pakke fra utlandet, men ble svindlet etter å ha fulgt en e-postlenke som angivelig var fra Posten. Nemndas flertall kom til at kunden ikke hadde handlet grovt uaktsomt. Selv om det var sider ved e-postens innhold og språkføring som var egnet til å vekke mistanke, var ikke dette nok for flertallet til å konkludere med at kunden hadde handlet grovt uaktsomt. Tilsvarende konkluderte nemndas flertall i en liknende sak i FinKN-2022-240, begrunnet med at det ikke er grovt uaktsomt «å unnlate å holde musepekeren over avsenderfeltet for å få frem den virkelige avsenderen». Denne linjen ble imidlertid ikke fulgt i FinKN-2022-242, der klager mottok en e-post som informerte om at det lå en pakke og ventet på henne, og at hun måtte betale 27 kroner for å få den tilsendt. Kunden ble deretter svindlet for i overkant av 10 000 kroner. Nemnda konkluderte med at kunden hadde handlet grovt uaktsomt, ettersom avsenderadressen tilsynelatende var fra Digipost og ikke Posten, e-posten bar preg av dårlig språkføring, og betalingsfristen på 13 dager var lengre enn leveringstiden for pakken, som skulle leveres innen 24 timer. Dette viser at konkrete forhold ved den enkelte e-posten fortsatt tillegges avgjørende vekt, selv om kunden skulle vente en tjeneste av nettopp den karakter e-posten omtaler.

I en sak fra mars 2023, FinKN-2023-188, kan det imidlertid se ut til at nemnda har senket terskelen for hva som anses som grovt uaktsomt, ytterligere. Saken gjaldt en e-post som utga seg for å være fra Skatteetaten. E-posten hadde synlig avsenderadresse: «yognuhiste@vusra.com». Nemndas flertall kom til at kunden ikke hadde opptrådt grovt uaktsomt, og uttalte i den forbindelse:

«Flertallet er enig med foretaket i at teksten i e-posten er formulert lite profesjonelt. Flertallet mener likevel at teksten ikke er så uprofesjonell at den uten videre måtte vekke

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

[81] Tilsvarende i FinKN-2021-1086.

mistanke. Avsenderadressen for e-posten er lite troverdig for en e-post fra Skatteetaten. Flertallet ser det slik at en mottaker av e-post ikke nødvendigvis henger seg opp i avsenderadressen når e-posten i seg selv ikke fremstår som utroverdig.»

Nemnda har med dette beveget seg langt fra utgangspunktet som ble slått fast i de første sakene i 2017 og 2018 om at det selv i tilfeller der det er vanskelig eller umulig å se at e-posten ikke er ekte, likevel er grovt uaktsomt å «la seg svindle».

Til sammenlikning kan praksis fra andre EU-land belyse hvordan de tilsvarende reglene er tolket i disse landenes respektive nasjonale lovgivning.[82] Vi kan eksempelvis se hen til Danmark og Storbritannia, som begge har implementert PSD 2 i nasjonal rett.[83] Sammenliknet med praksis fra disse landene virker tidligere praksis i Norge å følge en strengere aktsomhetsnorm i liknende saker. Nyere praksis er derimot mer på linje med slik reglene er anvendt i Storbritannia og Danmark.

Det finansielle ankenævn i Danmark konkluderte i sak 290/2018 at kunden ikke hadde handlet grovt uaktsomt. Kunden hadde 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 informasjon som gjorde det mulig for svindlerne å belaste kundens konto. Ankenævnet konkluderte med at kunden ikke hadde handlet grovt uaktsomt, ettersom henvendelsen samlet sett fremsto som troverdig. Dette var tilstrekkelig for ikke å anse handlingen som grovt uaktsom.

Heller ikke i Storbritannia konkluderer The Financial Ombudsman Service med grov uaktsomhet i liknende saker. I sak DRN-4082740 (22. desember 2020) 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.

Det samme ble resultatet i sak DRN-4139348 (2. juli 2020). Kunden hadde fått en e-post som ba ham 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» at det utgjorde grov uaktsomhet. Det slås uttrykkelig fast at det å dele

---

[82] Se Marte Eidsand Kjørven, «Who pays when things go wrong? Online financial fraud and consumer protection in Europe and Scandinavia», *European Business Law Review*, 2020, 31(1), s. 13 for en mer inngående komparativ analyse av praksis fra de skandinaviske landene.

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

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 Service har kommet til samme resultat.[84] Praksisen viser at de ikke anser det som grovt uaktsomt å falle for velgjennomført og profesjonell phising.

Gjennomgangen viser at nemndspraksis i Norge har gått nokså langt i å definere aktsomhetsnormen etter hvordan en idealkunde ville handlet, og dermed ikke har forholdt seg til utgangspunktet i Rt-2004-499 om at det er de kvalifisert klanderverdige tilfellene som faller under betegnelsen «grovt uaktsomme» pliktbrudd. Finansklagenemnda har ansett 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 unntaksvis og under helt spesielle omstendigheter har nemnda 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 angår phishing, etter min oppfatning ikke anses som uttrykk for en riktig vurdering 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 liknende henvendelser til sine kunder.

Nyere praksis, og særlig saken fra mars 2023, tyder imidlertid på et ytterligere taktskifte fra flertallet i nemnda. Etter min mening er denne saken i bedre samsvar med gjeldende rett. I skrivende stund er det ikke avklart om banken vil følge uttalelsen.[85]

7.4 Kan det være grovt uaktsomt å bli lurt til å oppgi sikkerhetsinformasjon muntlig til tredjepersoner?

I forlengelse av punktet ovenfor om phishing-svindel er det også relevant å spørre om det å falle for såkalt *vishing*-svindel er grovt uaktsomt. Som forklart innledningsvis er dette en særlig form for *phishing* der svindleren tar telefonisk kontakt med offeret. I Norge omtales dette gjerne som «Olga-svindel», ettersom ofrene for slik svindel ofte er eldre personer.

Disse sakene har som regel omhandlet grensen mellom grov uaktsomhet og forsett. Det vil si at kunden har akseptert å ha handlet grovt uaktsomt, men bestrider at pliktbruddet

[84] Se eksempelvis DRN-2174713 (15. september 2020), DRN-5688949 (26. april 2019) og DRN-4773354 (21. desember 2018).

[85] Uttalelser fra Finansklagenemnda er kun veiledende og har ikke bindende virkning.

var forsettlig.[86] Finansklagenemnda har i slike saker hovedsakelig konkludert med at kunden ikke har handlet forsettlig, ettersom kunden har vært i unnskyldelig rettsvillfarelse.[87]

Høyesterett har ved ett tilfelle avgjort en sak som omhandler Olga-svindel. I HR-2022-1752-A ble en kunde i en telefonsamtale, som angivelig var med kundens bank, lurt til å oppgi personlig sikkerhetsinformasjon knyttet til kundens BankID. Kundens konto ble deretter belastet for 240 336. Partene var enige om at kunden hadde handlet grovt uaktsomt; spørsmålet var om kunden hadde handlet *forsettlig*, jf. finansavtaleloven (1999) § 35 tredje ledd. Ettersom finansavtaleloven (1999) § 35 tredje ledd måtte forstås slik at «kunden må ha vore medviten om pliktbrotet for å kunne bli ramma» av bestemmelsen, og dette ikke var tilfellet i denne saken, konkluderte Høyesterett med at kunden ikke hadde handlet forsettlig.[88]

Hvorvidt kunden har handlet grovt uaktsomt i slike tilfeller, må underlegges de samme vurderinger som ved phishing-svindel som skjer ved bruk av e-post, sms eller liknende, se nærmere om dette i punkt 7.3. Som for phishing-svindel påvirkes skyldvurderingen av de faktiske omstendighetene i det konkrete tilfellet. Det er først og fremst nærliggende å trekke frem om svindleren utgir seg for å være en aktør som det er vanlig å oppgi personlig sikkerhetsinformasjon til. Eksempelvis vil det være mindre betenkelig å oppgi personlig sikkerhetsinformasjon til sin egen bank, ettersom det for den alminnelige bankkunde vil fremstå som usannsynlig at ens egen bank vil svindle dem.[89] På den annen side kan det være mer betenkelig å oppgi slik informasjon til andre aktører hvor det ikke er vanlig å gi slik informasjon – eksempelvis aktører som utgir seg for å være «tech-support».

Det kan være svært vanskelig å avsløre at en henvendelse ikke er reell. Et nummersøk vil ikke nødvendigvis hjelpe kunden, ettersom svindlere ved såkalt *spoofing* kan manipulere nummeret som ringer, slik at det fremstår som et annet. Dette kan tvert imot styrke kundens tro om at henvendelsen er reell. Henvendelsens innhold vil da være sentralt ved skyldvurderingen. Dersom svindleren utgir seg for å være kundens bank, er dette

---

[86] Se eksempelvis HR-2022-1752-A avsnitt 33.

[87] Se nærmere i Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 348 flg. Også nyere praksis fra Finansklagenemnda har fulgt samme argumentasjonslinje, se FinKN-2022-233, FinKN-2022-198 og FinKN-2022-197. Alle avgjørelsene er fra før HR-2022-1752-A, men avgjørelsene viser til lagmannsrettens dom i samme sak som på tidspunktet ikke var rettskraftig.

[88] HR-2022-1751-A avsnitt 50.

[89] Se Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 339 flg., hvor det gjøres nærmere rede for tolkningen av kundens avtalefestede plikt til ikke å oppgi personlig sikkerhetsinformasjon til uvedkommende, herunder banken eller politiet, og hvordan dette bør forstås ved skyldvurderingen.

ofte for å lure kunden til å tro at et lån blir utbetalt. Under det tidspresset kunden opplever, kan det fremstå rasjonelt at passord til BankID og engangskode oppgis for å få stanset utbetalingen av lånet. Slik som ved alminnelig innlogging i nettbanken, har dette karakter av å være en måte å identifisere seg overfor banken på.

Dersom kunden imidlertid oppgir informasjonen flere ganger, vil det gi en sterkere indikasjon på at det er tale om svindel. Etter omstendighetene vil antallet ganger det bes om at passord og engangskode oppgis, kunne være avgjørende for om pliktbruddet kategoriseres som grovt uaktsomt. Samtidig kan det i seg selv være en indikasjon på at det er tale om potensiell svindel, at kunden må oppgi betalingsinformasjon over telefon, ettersom det å oppgi denne informasjonen til en tredjeperson over telefon, ikke ligger innenfor det alminnelige bruksområdet til verken BankID eller betalingskort.

Dersom kontakten fremstår som om den er fra en reell aktør, og det ikke foreligger grunn til å reagere på innholdet i henvendelsen utover det faktum at svindleren har tatt kontakt over telefon, kan kunder utsatt for vishing-svindel ut fra omstendighetene ikke nødvendigvis sies å ha handlet grovt uaktsomt. Bærende for skyldvurderingen er den faktiske villfarelsen kunden er i under kontakten med svindleren.[90]

Det å uten videre akseptere at man har handlet grovt uaktsomt, er ikke heldig for kunden – selv om en reduksjon av ansvaret fra eksempelvis 240 336 til 12 000 kroner isolert sett er å regne som en «seier». Man skal imidlertid ikke undervurdere viktigheten av å rubrisere det enkelte svindeltilfellet under «riktig» skyldform. For det første kan dette danne presedens for hva som utgjør grov uaktsomhet, uten at det i realiteten skjer en skyldvurdering, også for andre former for svindel eller nye former for svindel. På denne måten legges mer av ansvaret på kunden, uten at pliktbruddet nødvendigvis faktisk utgjør grov uaktsomhet. For det andre kan dette medføre at tvistetemaet ofte vil være hvorvidt kunden har handlet forsettlig, ettersom kunden uansett har akseptert å ha handlet grovt uaktsomt. Slik kan grensen mellom grov uaktsomhet og forsett bli mer uklar ved nye og uprøvde former for svindel, selv om dette i prinsippet ikke skal ha betydning for vurderingen av hva som utgjør et forsettlig pliktbrudd.

8 Oppsummering og noen rettspolitiske betraktninger

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 elektroniske betalingsløsninger medfører.[91] Av den grunn må også ansvarsfordelingen mellom

[90] Se Kjørven Marte Eidsand Kjørven, Alf Petter Høgberg og Geir Woxholth, «BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4)», *Lov og Rett,* årg. 60, nr. 6, 2021, s. 351 flg. for en nærmere gjennomgang av betydningen av faktisk og rettslig villfarelse.

[91] PSD 2 fortalen punkt 7.

betalingstjenesteyteren og kunden innebære at tilliten 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.[92] 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. Kunden kan da som utgangspunkt ikke holdes ansvarlig for det økonomiske tapet. Av den grunn kan det også hevdes at digitaliseringen av betalingstjenester har medført et skifte i hvordan risikoen fordeles mellom kunden og betalingstjenesteyteren når svindel har funnet sted.[93]
Finansavtaleloven (2020) endrer ikke risikofordelingen som sådan, utover at kunden holdes ansvarlig for en objektiv egenandel som er mindre enn etter finansavtaleloven (1999). Ved tredjepersons misbruk av betalingskort og tilhørende kode tyder etterfølgende nemndspraksis på at terskelen for grov uaktsomhet stort sett har blitt praktisert på linje med Høyesteretts forutsetninger i Rt-2004-499. Enkeltavgjørelser viser at nemnda har lagt terskelen for grovt uaktsomme pliktbrudd høyere enn det tilsynelatende er grunnlag for, hvor begrunnelsen for at det foreligger grov uaktsomhet, både er utilstrekkelig og mangelfull. Enkeltavgjørelser fra Finansklagenemnda har imidlertid svært begrenset rettskildeverdi.

Særlig når det gjelder phishing, etablerte Finansklagenemnda over flere år en linje hvor terskelen for grov uaktsomhet ble satt såpass lavt at kunden nærmest ble holdt objektivt ansvarlig for en egenandel på 12 000 kroner dersom kunden hadde falt for slik svindel. Dette kan neppe anses å være i overensstemmelse med den terskelen for grov uaktsomhet som Høyesterett har trukket opp, selv om det i nyere praksis er en viss antydning til oppmykning av praksisen. Etter min oppfatning har kunden i nemndspraksis blitt målt 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 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, er det svært strengt når kunden har blitt holdt ansvarlig for grovt uaktsomme pliktbrudd når meldingen ellers med ganske høy grad av presisjon illuderer

[92] EU-kommisjonen. «A digital single Market Strategy for Europe». *SWD,* 2015, 100, s. 51.

[93] Marte Eidsand Kjørven, «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. 104.

en reell henvendelse. En helt fersk avgjørelse fra mars 2023 synes å innebære et taktskifte.

Om Finansklagenemnda hittil har ansett egenandelen etter finansavtaleloven (1999) på 1200 kroner som for lav og av den grunn konkludert med grov uaktsomhet i mange av phishing-sakene, vil dette medføre en tilsidesettelse av lovgivers intensjon der nemnda egenhendig og ubegrunnet har utvidet kundens egenandel til 12 000 kroner.

Ettersom tvistesummen i disse sakene er begrenset til 12 000 kroner, er domstolene lite tilgjengelige. Å føre en sak for domstolene er en kostbar prosess, og omkostningene vil nesten uten unntak overgå tvistesummen, idet kunden risikerer å sitte igjen med regningen for både sin egen og motpartens advokat i tillegg til egenandelen. Dette gjør det problematisk å få disse sakene inn til behandling i domstolene. Finansklagenemnda blir av den grunn det eneste reelle tvisteløsningsorganet i det store flertallet av disse sakene. Det er derfor gledelig at nemnda nå kan se ut til å ha realitetsorientert seg både med tanke på de rettslige utgangspunktene for fastleggelse av terskelen for grov uaktsomhet og hva man faktisk kan forvente av enkeltpersoner med tanke på å avdekke svindelforsøk.