Ansvaret for uautoriserte betalingstransaksjoner

Særlig om grensen mellom simpel og grov uaktsomhet ved misbruk av elektroniske betalingsinstrumenter

Kandidatnummer: 9

Antall ord: 14 362

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

1. juni 2018

Innholdsfortegnelse

Innholdsfortegnelse 2
1 Innledning 4
1.1 Problemstilling 4
1.2 Temaets aktualitet og sentrale hensyn 5
1.3 Rettskilder, metode og avgrensning 7
1.4 Veien videre 9
2 Nærmere om vilkårene i finansavtaleloven §§ 34 og 35 11
2.1 Innledning 11
2.2 Kunden har ikke gitt «samtykke» til transaksjonen 12
2.3 Kundens ansvar for egenandel inntrer bare ved bruk av «betalingsinstrument» 14
2.4 Forskjeller i vilkårene for å subsumere tilfellet under henholdsvis finansavtaleloven § 35 andre og tredje ledd 16
2.5 Nærmere om forpliktelsene etter finansavtaleloven § 34 første ledd 19
3 Uaktsomhetsvilkåret 21
3.1 Innledning 21
3.2 Innholdet i uaktsomhetsvilkåret 21
3.2.1 Norge 21
3.2.2 Komparativt: uaktsomhetsvilkårets innhold i svensk og dansk rett 23
4 Analyse av typetilfeller der spørsmålet er om kunden har opptrådt grovt uaktsomt 24
4.1 Kamuflasje av PIN-koden 24
4.1.1 Innledning 24
4.1.2 Grensen mellom simpel og grov uaktsomhet i norsk rett 24
4.1.3 Komparativt 28
4.2 Tyveri fra hotellrom eller annet midlertidig bosted 29
4.2.1 Grensen mellom simpel og grov uaktsomhet i norsk rett 29
4.2.2 Komparativt 30
4.3 Tyveri fra privat hjem 32
4.3.1 Grensen mellom simpel og grov uaktsomhet i norsk rett 32
4.3.2 Komparativt 33
4.4 Tyveri fra bil 35
4.4.1 Grensen mellom simpel og grov uaktsomhet i norsk rett 35

4.4.2 Komparativt 36
4.5 Lekkasje av PIN-koden 38
4.5.1 Innledning 38
4.5.2 Grensen mellom simpel og grov uaktsomhet i norsk rett 39
4.5.3 Komparativt 41
4.6 Bruk av mobiltelefon eller nettbrett til å gjennomføre uautoriserte betalingstransaksjoner 42
4.6.1 Innledning 42
4.6.2 Overlatelse av instrumentet til andre 43
4.6.3 Lekkasje av PIN-koden 46
4.6.4 Oppbevaring av betalingskort og mobiltelefon sammen 46
5 Avslutning 48
Litteraturliste 50

1 Innledning

1.1 Problemstilling

Temaet for oppgaven er innholdet og praktiseringen av reglene om misbruk av konto og betalingsinstrument i finansavtaleloven § 35.[1] Bestemmelsen plasserer det økonomiske ansvaret for uautoriserte betalingstransaksjoner helt eller delvis på finansinstitusjonen eller på kontohaver. Utgangspunktet etter finansavtaleloven § 35 første ledd er at institusjonen er ansvarlig for tap som oppstår som følge av uautoriserte betalingstransaksjoner. Paragraf 35 andre og tredje ledd slår imidlertid fast at kunden i visse tilfeller må bære hele eller deler av tapet selv. Etter andre ledd svarer kunden på visse vilkår for inntil 1.200 kroner når tapet skyldes bruk av et tapt eller stjålet betalingsinstrument, for eksempel betalingskort.[2] Videre svarer kunden for hele tapet dersom han ved grov uaktsomhet har unnlatt å følge nærmere bestemte forpliktelser i § 34 første ledd, jf. § 35 tredje ledd.[3] Dersom betalingsinstrumentet som er misbrukt er elektronisk, gjelder imidlertid en ansvarsbegrensning for kunden på 12.000 kroner. Dette innebærer at et misbruk som er skjedd ved bruk av papirgiro eller sjekk vil føre til at kunden hefter for hele summen, mens han kun hefter for inntil 12.000 kroner når misbruket er skjedd ved bruk av betalingskort.[4]

Den rettslige problemstillingen for oppgaven er hvordan ansvaret skal fordeles mellom finansinstitusjonen og kunden når tredjeperson har gjennomført uautoriserte betalingstransaksjoner ved bruk av kundens betalingsinstrument. En tilleggsproblemstilling er om svensk og dansk rett praktiserer reglene om fordeling av ansvaret mellom institusjonen og kunden på samme måte som i norsk rett.

Oppgaven skal særlig fokusere på grensen mellom simpel og grov uaktsomhet etter henholdsvis finansavtaleloven § 35 andre og tredje ledd. Dette er fordi vurderingen av om

[1] Lov av 25. juni 1999 om finansavtaler og finansoppdrag.
[2] Se kapittel 2.4 for nærmere redegjørelse.
[3] Se nærmere om dette i kapittel 2.
[4] Ot.prp.nr.94 (2008-2009) s. 185.

kunden har opptrådt grovt uaktsomt er den mest prosessdrivende og praktisk viktigste vurderingen knyttet til uautoriserte betalingstransaksjoner.[5] Årsaken til at denne vurderingen er den viktigste er fordi grov uaktsomhet innebærer at kunden må dekke en mye større del av tapet selv enn dersom han ikke har opptrådt grovt uaktsomt. Videre er grov uaktsomhet en rettslig standard, slik at begrepets innhold ikke er å finne i loven selv.[6] Med unntak av at begrepet selv gir rettsanvenderen en viss veiledning, vil innholdet av en rettslig standard bero på en normativ vurdering.[7] Det nærmere innholdet av vilkåret må dermed fastlegges i praksis, noe som gjør grensedragningen mellom hva som anses som henholdsvis simpel og grov uaktsomhet interessant. Oppgaven skal ha et blikk mot de tilsvarende reglene og praktiseringen av disse i svensk og dansk rett av grunner som er nærmere beskrevet i kapittel 1.3.

1.2 Temaets aktualitet og sentrale hensyn

En uautorisert betalingstransaksjon er i finansavtaleloven § 35 første ledd jf. § 12 bokstav a definert som en «handling [...] for å innbetale, overføre eller ta ut midler, uten hensyn til underliggende forpliktelser mellom betaleren og betalingsmottakeren», uten samtykke fra kunden. Det er altså tale om alle handlinger der kundens konto blir belastet uten at kunden har akseptert belastningen.

Forutsetningen for å plassere ansvaret på finansinstitusjonen eller kunden er at den som har gjennomført transaksjonen er ukjent eller av andre grunner ikke kan stilles til ansvar for misbruket. Spørsmålet etter å ha konstatert at det er gjennomført en uautorisert betalingstransaksjon blir dermed om det er banken eller kunden som har det økonomiske ansvaret for tredjepersonens handling. Denne forutsetningen om en tredjeperson skiller reglene om misbruk av konto og betalingsinstrument fra den øvrige kontraktsretten ved at tre parter er involvert i stedet for de tradisjonelle topartsforholdene.

[5] Se https://publisering.finkn.no/keywords/4/AZ0101 (sist besøkt 26.04.2018). 604 av 1142 kortsaker dreier seg om grov uaktsomhet fra kundens side.
[6] Sundberg (1984) s. 659.
[7] Ibid. s. 661-662.

Uautoriserte betalingstransaksjoner har vært et samfunnsproblem i flere tiår, og med den teknologiske utviklingen har risikoen blitt større. Tyveri og misbruk av bankkort er i dag det rådende problemet når det gjelder uautoriserte transaksjoner.[8] Utviklingen i teknologien bidrar utvilsomt til sikrere betalingsløsninger enn før, men nye teknologiske løsninger vil også gjøre det enklere å misbruke betalingsinstrumenter.[9] Dette gjelder for eksempel kontaktløs betaling med kort og mobile betalingsinstrumenter som Vipps. Det er derfor grunn til å vente at problemet med uautoriserte betalingstransaksjoner vil øke i fremtiden. Med stadig økende reisevirksomhet og en kontinuerlig teknologisk utvikling, er det særlig de eldre som fremstår som den største risikogruppen i fremtiden.[10] Men også yngre personer vil bli utsatt for en større risiko, fordi det er blitt enklere å skaffe seg tilgang til betalingsinstrumentene som benyttes. For kontaktløse kort kreves kun at man har fått tilgang til selve kortet; verken PIN-kode eller signatur er nødvendig.

Det er heller ikke vanskelig å få tilgang til andre personers mobiltelefoner, som kan fungere som betalingsinstrumenter; de siste årene har aktører som mCash, Mobilepay og Vipps by DnB hatt stor suksess med alt fra vennebetalinger til kjøp av varer i butikk via mobiltelefon. I dag står kun Vipps igjen i det norske markedet.[11] Fremstillingen vil i det følgende derfor begrense seg til dette produktet når den behandler spørsmål som er knyttet til mobile betalingsinstrumenter.

Fordi reglene skal ta høyde for både tredjepersonsproblemet og den stadige utviklingen i betalingsformidlingen, er det nødvendig å si noe om de ulike motstående hensyn som ligger til grunn for plasseringen av ansvaret. Pulveriseringshensynet taler i retning av å plassere ansvaret hos finansinstitusjonen, idet det økonomiske tapet vil bli pulverisert på alle kundene hos institusjonen.[12] Samtidig vil ansvaret gi institusjonene incentiv til å lage sikre

[8] https://publisering.finkn.no/keywords/4/AZ01 (sist besøkt 13.02.2018), der mer enn 800 saker gjelder misbruk av bankkort alene.
[9] https://e24.no/lov-og-rett/bank/rekordaar-for-kortsvindel-i-2016-over-17-milliarder-tapt-i-europa/24095074 (sist besøkt 22.03.2018).
[10] https://www.nrk.no/buskerud/_kan-jeg-fa-pin-koden-din__-1.11834850 (sist besøkt 21.03.2018) og https://dnbfeed.no/privatokonomi/unnga-a-bli-lurt-eller-svindlet/ (sist besøkt 22.03.2018).
[11] https://www.aftenposten.no/okonomi/i/Pk2k0/Alle-bankene-er-snart-med-i-Vipps (sist besøkt 21.03.2018).
[12] Ot.prp.nr.94 (2008-2009) s. 128.

betalingsordninger, slik at det blir vanskelig å misbruke betalingsinstrumenter selv om det oppstår stadig nye måter å misbruke betalingsinstrumenter på.[13]

Motsatt må også forbrukeren ha oppfordring til å behandle betalingsinstrumentene på en slik måte at det ikke blir misbrukt, på tross av at tilgangen til enkelte betalingsinstrumenter, og dermed muligheten til å misbruke instrumentene, er blitt enklere.[14] En slik oppfordring får kunden gjennom å måtte betale egenandelen på 1.200 kroner dersom vilkårene i § 35 andre ledd er oppfylt, og 12.000 kroner dersom han har opptrådt grovt uaktsomt med hensyn til et elektronisk betalingsinstrument. Disse reglene søker å balansere de ulike hensynene, samtidig som lovgiver anerkjenner at risikoen for å bære den største delen av tapet bør ligge hos den profesjonelle parten.

1.3 Rettskilder, metode og avgrensning

Oppgaven tar utgangspunkt i finansavtaleloven § 35 andre og tredje ledd. Denne bestemmelsen gjennomfører betalingstjenestedirektiv 1 (PSD 1) artikkel 59, som slår fast at kunden i utgangspunktet kommer i ansvar for den uautoriserte transaksjonen der kunden har utvist «grov forsømmelse».[15] PSD 2 opphever PSD 1, og det er gjennomført flere endringer i reglene knyttet til uautoriserte betalingstransaksjoner i det nye direktivet.[16]

Det nye direktivet er kun gjennomført i EU, og ikke EØS, men Norge ventes å gjennomføre de privatrettslige aspektene av PSD 2 i nær fremtid gjennom vedtakelsen av en ny finansavtalelov.[17] Selv om det er gjort endringer i reglene om uautoriserte betalingstransaksjoner fra PSD 1 til PSD 2, vil endringene i det nye direktivet ikke påvirke direkte det som skal behandles i oppgaven. Dermed vil innholdet i denne oppgaven ikke bli

[13] Ibid. s. 125 og fortalen til PSD 2, avsnitt 95.
[14] Ot.prp.nr. 94 (2008-2009) s. 128.
[15] EP/Rdir 2007/64 EF.
[16] EP/Rdir (EU) 2015/2366.
[17] Snr. 17/4746 Høringsnotat – revisjon av finansavtaleloven.

rettshistorie ved den forestående gjennomføringen av PSD 2, men fortsatt være relevant. På bakgrunn av dette vil oppgaven derfor vise til PSD 1 når direktivet er relevant.

Medlemsstatene i EU, i tillegg til Norge, velger selv hvordan og i hvilken form direktivet gjennomføres.[18] Når Norge har valgt å gjennomføre direktivet ved transformasjon, kan det oppstå språklige forskjeller mellom direktivet og finansavtaleloven. Finansavtaleloven må derfor tolkes EØS-konformt etter alminnelig norsk juridisk metode med mindre det er klar motstrid mellom loven og direktivet.[19] Tolkningen av direktivreglene må følge den mer formålsrettede metoden som EU-domstolen bruker.[20]

EU-samarbeidet tilstreber rettsenhet innenfor de områdene samarbeidet omfatter.[21] Det er likevel en stor utfordring å skape rettsenhet på tvers av landegrenser, og det er ikke gitt at medlemslandene i EU har en lik forståelse av hvordan ansvaret skal fordeles mellom institusjon og kunde. Det er imidlertid klart at Norge, Sverige og Danmark har relativt like rettssystemer og -kulturer, slik at det derfor er av interesse å undersøke hvorvidt de tre skandinaviske landene fordeler ansvaret for uautoriserte transaksjoner likt mellom finansinstitusjonen og forbrukeren.

Sverige og Danmark har gjennomført PSD 2 i den nasjonale lovgivningen. I Sverige er dette gjort i lagen om obehöriga transaktioner 4 og 6 §§.[22] Danmark har vedtatt en ny betalingslov som gjelder fra 1. januar 2018, der man finner de relevante bestemmelsene i §§ 97-100.[23] Det er ingen praksis i dansk rett knyttet til denne loven enda, men det er ikke funnet holdepunkter for at det er foretatt noen realitetsendringer med tanke på det som skal behandles i denne oppgaven. Derfor brukes bare den någjeldende betalingsloven når det er nødvendig å vise til nasjonal lovgivning.

[18] TEUV art. 288.
[19] Sejerstedt, Arnesen, Foyn mfl. (2011) s. 250 ff.
[20] Ibid. s. 468.
[21] TEU art. 3 nr. 3 (3).
[22] Lag (2010:738) om obehöriga transaktioner med betalingsinstrument.
[23] Lov nr. 652 af 8. juni 2017 om betalinger.

Et særtrekk ved tvister som gjelder misbruk av betalingsinstrumenter i de tre nasjonene som behandles her er at alle har en egen nemnd som behandler tvistene. Selv om disse avgjørelsene ikke har bindende virkning vil dermed kun et fåtall av sakene komme opp for domstolene, og nesten ingen vil bli prosedert for Høyesterett.[24] På grunn av den begrensede rettspraksisen vil denne fremstillingen også inneholde lite rettspraksis, men oppgaven behandler likevel det meste av rettspraksis som er knyttet til tvister angående grov uaktsomhet. Praksis fra nemndene vil dermed få et stort fokus i den juridiske analysen. Selv om avgjørelser avsagt i Finansklagenemnda ikke hører til det samme rettskildemessige hierarkiet som ordinære domstolsavgjørelser, er det akseptert at nemndspraksis har rettskildemessig verdi.[25] I tillegg vil en fast og langvarig praksis fra nemnda kunne nyte en større anerkjennelse enn enkeltstående avgjørelser.[26]

Oppgaven skal fastlegge hva som er gjeldende rett innenfor problemstillingen, og dermed vil den rettsdogmatiske metoden brukes gjennomgående i oppgaven. I de komparative avsnittene vil oppgaven imidlertid bruke komparativ metode.

Det er også nødvendig å si noe kort om avgrensninger i oppgaven. Fordi PSDs bestemmelser om uautoriserte transaksjoner kun er ufravikelige overfor forbrukere, vil oppgaven avgrense mot uautoriserte transaksjoner der næringsdrivende er rammet.[27] Analysen vil også avgrense mot betalingsinstrumenter som ikke er elektroniske, fordi elektroniske betalingsinstrumenter er de mest brukte.

1.4 Veien videre

I den videre fremstillingen vil kapittel 2 gjennomgå de viktigste vilkårene i finansavtaleloven §§ 34 og 35, og i hvilken grad disse kommer til anvendelse for ulike typer

[24] Saksbehandlingsregler for Finansklagenemnda, punkt 14. Se også Ot.prp.nr.41 (1998-1999) s. 90.
[25] Krüger (2008) s. 116 og 118 med videre henvisninger. Tilsvarende Ot.prp.nr.41 (1998-1999) s. 87.
[26] Krüger (2008) s. 116.
[27] Se PSD 1 artikkel 51 nr. 1, som slår fast at artikkel 61 om kundens ansvar ved grov forsømmelse kan fravikes der kunden ikke er en forbruker og Ot.prp.nr.94 (2008-2009) s. 120.

betalingsinstrumenter. Det blir også knyttet enkelte kommentarer til §§ 24, 24a og 26 om krav til samtykke til en transaksjon. Kapittel 3 fastlegger innholdet i vilkåret om grov uaktsomhet etter § 35, både etter norsk, svensk og dansk rett.

Kapittel 4 inneholder en analyse av grensen mellom simpel og grov uaktsomhet ved uautoriserte transaksjoner ved bruk av praksis fra domstolene og Finansklagenemnda. Her vil det også bli supplert med praksis fra den svenske Allmänna Reklamationsnemnden og det danske Pengeinstitutankenævnet. Kapitlet vil avslutte med å analysere grensen mellom simpel og grov uaktsomhet ved uautoriserte transaksjoner som er gjennomført på applikasjonen Vipps. Avsluttende merknader kommer i kapittel 5.

2 Nærmere om vilkårene i finansavtaleloven §§ 34 og 35

2.1 Innledning

Hvorvidt det er forbrukeren eller banken som har ansvaret for en uautorisert transaksjon, beror på en rekke vilkår i finansavtalelovens § 34 første ledd, og § 35 andre og tredje ledd. En transaksjon er uautorisert kun dersom kunden ikke har gitt «samtykke» til transaksjonen. Dermed skal det først klarlegges hva som utgjør et «samtykke» i kapittel 2.2. Deretter skal begrepet «betalingsinstrument» tolkes i kapittel 2.3.

Videre er det forskjeller i hvilke vilkår som gjelder for simpel uaktsomhet og aktsom opptreden i § 35 andre ledd og den grove uaktsomheten i tredje ledd. For at andre ledd skal komme til anvendelse må det først være tale om bruk av «personlige sikkerhetsanordninger». Deretter følger to alternative grunnlag for at kunden hefter for noe av tapet, som begge forutsetter bruk av disse sikkerhetsanordningene. Det første grunnlaget er at betalingsinstrumentet er «tapt eller stjålet». Det andre grunnlaget krever at betalingsinstrumentet er «uberettiget [tilegnet]» og kunden har «mislyktes» i å beskytte de personlige sikkerhetsanordningene. Alle disse vilkårene skal det gjøres rede for i kapittel 2.4.

Til slutt skal det i kapittel 2.5 ses nærmere på forpliktelsene kunden er underlagt etter § 34 første ledd. Bestemmelsen krever at kunden bruker betalingsinstrumentet «i samsvar med vilkårene for utstedelse og bruk» og at alle «rimelige forholdsregler» for å beskytte sikkerhetsanordningene blir tatt i bruk. Videre må kunden «uten ugrunnet opphold» varsle banken dersom han blir oppmerksom på «tap, tyveri eller uberettiget tilegnelse av betalingsinstrumentet, eller på uautorisert bruk».

2.2 Kunden har ikke gitt «samtykke» til transaksjonen

Etter finansavtaleloven §§ 24 andre ledd og 35 første ledd er banken bare ansvarlig for en betalingstransaksjon i de situasjonene der kunden ikke har gitt «samtykke» til den. Bestemmelsen gjennomfører PSD 1 artikkel 54 nr. 1 og nr. 2 andre ledd, som også slår fast at en transaksjon uten «samtykke» er uautorisert.[28]

Hvordan vilkåret skal tolkes i direktivet, finnes det imidlertid få EU-rettslige kilder på, foruten ordlyden og formålet med bestemmelsen. Ordlyden peker mot at kunden gjennom ord eller handling godkjenner at transaksjonen gjennomføres. Det finnes ingen uttalelser om formålet med bestemmelsen, men det er likevel liten tvil om at formålet er å sikre at en transaksjon ikke blir gjennomført uten visshet om at det er ønsket av kontohaver. Uttrykkelig godkjenning av transaksjonen er kjerneeksempelet på et samtykke som imøtekommer både ordlyden og formålet. Et uttrykkelig samtykke kan for eksempel være å taste inn PIN-koden på en betalingsterminal, eller godkjenne en transaksjon gjennom å iverksette en betalingsordre på nettbanken.[29]

Det kan tenkes at kunden etter omstendighetene har samtykket til transaksjonen ved passivitet.[30] Dette kan for eksempel være at kundens sønn låner betalingskortet til å kjøpe noe eller gjøre uttak med kundens viten, uten at kunden protesterer. Hvis slik passivitet anses som samtykke kan ikke kunden gjøre innsigelser mot banken i etterkant av transaksjonene. Juridisk teori knyttet til PSD 1 er imidlertid skeptisk til en slik ordning, fordi direktivet krever at det skal inngås en avtale mellom forbruker og institusjon om prosedyren for et slikt samtykke.[31]

[28] Ot.prp.nr.94 (2008-2009) s. 179. Ny relevant artikkel i PSD 2 er artikkel 64, men det er ingen realitetsendringer knyttet til denne artikkelen.
[29] Jf. også Grøttjord/Rosén (2014) s. 149.
[30] Giertsen (2014) s. 55-56.
[31] Geva (2009) s. 725. Her er ingen realitetsendringer knyttet til PSD 2.

I de fleste tilfeller vil en slik passivitet anses som et forsettlig brudd på kundens forpliktelser eller meldeplikten etter finansavtaleloven § 34 første ledd.[32] Dermed vil forbrukeren uansett hefte for tapet i disse tilfellene. En annen måte å samtykke til en betalingstransaksjon på er såkalte belastningsfullmakter etter finansavtaleloven § 26, mest kjent som avtalegiro, der institusjonen gjennomfører gjentatte transaksjoner på faste beløp til faste tidspunkt.

Et samtykke kan begrense seg både til transaksjonen som sådan, og til transaksjonens beløp.[33] Det førstnevnte tilfellet reguleres av finansavtaleloven § 24 andre ledd. Utgangspunktet er at en betalingstransaksjon kun er autorisert dersom det foreligger samtykke «før transaksjonen gjennomføres». Det følger imidlertid av § 24 siste punktum at også et etterfølgende samtykke kan autorisere transaksjonen, dersom dette er avtalt mellom kunden og banken. Siden kunden må reklamere på transaksjonen etter finansavtaleloven § 37 for å få pengene tilbake, kan det tenkes at transaksjoner blir autorisert etter at de er gjennomført selv uten en slik avtale. Dersom kunden senere ombestemmer seg, og banken ikke har en slik avtale å vise til, vil banken imidlertid bli ansvarlig til tross for samtykket, jf. lovens ordlyd. Kundens adgang til å reklamere etter å ha oppdaget transaksjonen er imidlertid tidsmessig begrenset etter finansavtaleloven § 34 første ledd.

Betalingstransaksjoner kan også være uautoriserte basert på transaksjonsbeløpet etter finansavtaleloven § 24a. Når første ledd bestemmer at det kan avtales belastningsgrenser for bruk av betalingsinstrumenter «som benyttes til å samtykke til en transaksjon», vil enhver overskridelse av denne belastningsgrensen være uautorisert.[34] Slike belastningsgrenser avtales ofte på tidsmessig basis, for eksempel pr. uke eller pr. måned.[35] Denne ordningen er praktisk for eksempel når mindreårige går til anskaffelse av betalingskort.[36] Dersom kortet har en belastningsgrense på 5.000 kroner og kortet er belastet for totalt 5.500 kroner innenfor den aktuelle tidsperioden, er 500 kroner av transaksjonen uautorisert.

[32] Se nærmere om forpliktelsene i kapittel 2.5.
[33] Krüger, Rettsdata, Finansavtaleloven, note (215).
[34] Tilsvarende Grøttjord og Rosén (2014) s. 151.
[35] Ibid. s. 152.
[36] Krüger, Rettsdata, Finansavtaleloven, note (131).

Tidligere utgjorde belastningsgrensene også ansvarsbegrensninger for kunden, men denne ordningen ble fjernet med den gjeldende finansavtaleloven.[37] Kundens objektive ansvar på inntil 1.200 kroner for uautoriserte transaksjoner etter finansavtaleloven § 35 andre ledd gjelder dermed fortsatt der PIN-koden er brukt og kortet er stjålet.[38] Siden det kun er summen over beløpsgrensen som er uautorisert, må beløpsgrensen overstiges med mer enn 1.200 kroner for at banken skal bli erstatningsansvarlig.

Det kan innvendes at en kunde som belaster instrumentet med en sum som overstiger belastningsgrensen, har gjort dette med vilje og dermed likevel har samtykket til transaksjonen. Forarbeidene er imidlertid klare på at banken uansett har ansvaret.[39] Poenget med disse belastningsgrensene er at finansinstitusjonen tar ansvaret for å begrense belastningene når kunden har behov for å sette grenser. Det kan for eksempel være at kunden syns det er vanskelig å ha oversikt over hvor mye han bruker, eller kunden sliter med overforbruk og ønsker hjelp til å begrense seg. Etter min mening er det derfor uten betydning at kunden med vilje overskrider belastningsgrensene.

2.3 Kundens ansvar for egenandel inntrer bare ved bruk av «betalingsinstrument»

Forutsetningen for at kunden hefter for egenandelen på 1.200 kroner eller 12.000 kroner etter henholdsvis finansavtaleloven § 35 andre og tredje ledd, er at tapet må skyldes bruk av et «betalingsinstrument». Begrepet er legaldefinert i § 12 bokstav c, og omfatter alle «personlige instrument eller sett av prosedyrer [...] som kunden benytter for å iverksette en betalingsordre». Dette tilsier at alle former for å gjennomføre en betaling, uttak, eller overføring av penger fra en konto er omfattet av bestemmelsen, slik at definisjonen favner svært bredt og omfatter blant annet sjekk, giro og betalingskort. Siden instrumentet er

[37] Ot.prp.nr.94 (2008-2009) s. 179.
[38] Se kapittel 2.3 for nærmere redegjørelse.
[39] Ot.prp.nr.94 (2008-2009) s. 123 og 130.

«personlig», må det kunne knyttes til en bestemt person, slik at for eksempel betalingskuponger ikke anses som betalingsinstrument.[40]

Hos noen banker er det nødvendig med kode fra BankID-brikken for å iverksette en betalingsordre i nettbanken. EU-domstolen har uttalt at direktivet må tolkes slik at «both the procedure for ordering transfers by means of a transfer order form signed by the payer in person and the procedure for ordering transfers through online banking constitute payment instruments within the meaning of that provision».[41] Tilsvarende synspunkter er gjort gjeldende i norsk juridisk teori.[42] Dermed vil også BankID etter omstendighetene kunne regnes som betalingsinstrument.

Et særlig spørsmål som angår Vipps er om applikasjonen som sådan er et betalingsinstrument etter finansavtaleloven § 12 bokstav c, eller om det kun er et middel for å benytte betalingskort som betalingsinstrument.[43] Det passer godt med ordlyden i § 12 å la Vipps være omfattet av definisjonen. Det er tale om et «personlig instrument» i form av en personlig profil, som benyttes til å «iverksette betalingstransaksjoner». Instrumentet har også grunnlag i en avtale mellom forbrukeren og institusjonen. Videre har Markedsrådet uttalt at «mobiltelefon er å anse som betalingsinstrument i finansavtalelovens forstand, når den [...] brukes til å iverksette en betalingsordre».[44]

Også EU-kommisjonen og forarbeidene til finansavtaleloven mener at en mobiltelefon kan fungere som betalingsinstrument.[45] Det kan også synes som at DnB selv mener at Vipps er et selvstendig betalingsinstrument; i vilkårene for bruk av Vipps heter det i punkt 6.4 at bruk av en «jailbreaket» telefon regnes som «alvorlig brudd på vilkårene for bruk av Vipps som betalingsinstrument».[46] Vipps er dermed et selvstendig betalingsinstrument. Dette innebærer

[40] Grøttjord/Rosén (2014) s. 94.
[41] Case C-616/11 T-Mobile Austria GmbH v Verein für Konsumenteninformation 9. april 2014 avsnitt 44.
[42] Grøttjord/Rosén (2014) s. 94.
[43] Nærmere om hvordan applikasjonen fungerer i kapittel 4.6.1.
[44] MR-2015-1018, pkt. 4.2.2.
[45] Jf. http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq-2008_11_20_en.pdf (sist besøkt 13.03.2018) og Ot.prp.nr.94 (2008-2009) s. 171.
[46] https://www.vipps.no/vilkar/vilkar-privat (sist besøkt 21.03.2018).

at det også er et «elektronisk betalingsinstrument» etter § 35 tredje ledd, slik at den øvre egenandelen på 12.000 kroner ved grov uaktsomhet gjelder ved misbruk av Vipps.

2.4 Forskjeller i vilkårene for å subsumere tilfellet under henholdsvis finansavtaleloven § 35 andre og tredje ledd

Finansavtaleloven § 35 andre ledd stiller opp to alternative grunnlag for at kunden skal hefte med 1.200 kroner av tapet. Felles for begge grunnlagene er at det må gjelde misbruk av et betalingsinstrument som definert i kapittel 2.2, og at de «personlige sikkerhetsanordningene» må ha vært brukt ved misbruket. Den språklige forståelsen av vilkåret tilsier at det må være tale om bruk av PIN-kode knyttet til et betalingskort, fingeravtrykk, eller andre biometriske data siden disse er personlige. Det følger imidlertid av forarbeidene at sikkerhetsanordninger som er personavhengige, slik som biometriske data, ikke er omfattet fordi man som regel ikke får tilgang til disse dataene uten å være berettiget.[47] Videre vil sikkerhetsanordninger som CVC-nummer falle utenfor bestemmelsens rekkevidde fordi nummeret står på kortet, og er dermed ikke personlig.[48] Dette medfører at ikke alle betalingsinstrumenter er omfattet av bestemmelsen; bruk av sjekk eller papirgiro krever for eksempel ikke bruk av noen sikkerhetsanordninger. Heller ikke misbruk av betalingskort der transaksjonen godkjennes med signatur omfattes av andre ledd, fordi signatur ikke er en sikkerhetsanordning, men en legitimasjonsordning. For disse betalingsinstrumentene må man dermed gå inn i en vurdering av tredje ledd. Hvis heller ikke dette fører frem, er banken ansvarlig for tapet fullt ut etter første ledd.

Et spørsmål er om Vipps er et betalingsinstrument med eller uten «personlige sikkerhetsanordninger». All informasjon som kreves for å gjennomføre en transaksjon på Vipps står oppført på betalingskortet. Dermed kreves ingen «personlige sikkerhetsanordninger» for å autorisere en transaksjon, slik som for bankkort. Det kreves imidlertid PIN-kode for å logge seg inn på Vipps. Ordlyden i § 34 krever at

[47] Ot.prp.nr. 94 (2008-2009) s. 118.
[48] Grøttjord/Rosén (2014) s. 204-205

sikkerhetsanordningen må være «knyttet til» betalingsinstrumentet. Dette tilsier at sikkerhetsanordningen ikke er nødt til å gjennomføre selve transaksjonen, så lenge anordningen har noe med betalingsinstrumentet å gjøre. PIN-koden for å logge inn på Vipps må derfor anses som en «personlig sikkerhetsanordning».

Enkelte mobiltelefoner tillater også bruk av fingeravtrykk for å logge inn, noe som klart ikke er en sikkerhetsanordning, jf. ovenfor.[49] Begrunnelsen for dette er at man «som utgangspunkt ikke vil få tilgang til systemene uten å være berettiget».[50] Denne begrunnelsen gjør seg ikke like gjeldende for mobiltelefoner, ettersom det er mulig å få tilgang ved for eksempel å slå eieren av enheten bevisstløs eller benytte seg av muligheten mens eieren sover. Forarbeidene er likevel klare på dette punkt, og formuleringen «som utgangspunkt» antyder at departementet har vurdert at det kan tenkes unntak, men at regelen fortsatt skal gjelde. Etter dette gjelder finansavtaleloven § 35 andre ledd ved uautorisert bruk av Vipps når innlogging skjer ved bruk av PIN-kode, men ikke når innlogging gjøres ved bruk av fingeravtrykk.

Det første alternative grunnlaget kommer til anvendelse når betalingsinstrumentet er «tapt eller stjålet» og de personlige sikkerhetsanordningene er brukt. Dette er det klart mest praktiske alternativet, ettersom de fleste misbruk skjer med fysiske betalingsinstrumenter som er fravendt eieren av instrumentet, eller som eieren har mistet.[51] Det stilles ingen krav til uaktsomhet i lovteksten, slik at ansvaret for egenandelen er objektivt.[52] Det andre alternativet er at betalingsinstrumentet har blitt «uberettiget [tilegnet]» og kunden har «mislyktes» i å beskytte de personlige sikkerhetsanordningene. Selv om ordlyden isolert sett peker mot andre former for fysisk fravendelse av instrumentet enn tyveri og tap, følger det av forarbeidene at dette alternativet omfatter betalingsinstrumenter som ikke «fysisk har kommet på avveie fra kunden ved tap eller tyveri».[53] Videre peker «mislyktes» mot at det ikke gjelder noe

[49] www.vipps.no/sporsmal - «Kan alle logge seg inn med Touch ID på iPhone eller fingeravtrykk på Android?» (Sist besøkt 12.03.2018).
[50] Ot.prp.nr.94 (2008-2009) s. 118.
[51] https://publisering.finkn.no/keywords/4/AZ01 (sist besøkt 21.02.2018), der det fremgår at nærmere 800 av 1142 kortsaker gjelder tap av kort.
[52] Grøttjord/Rosén (2014) s. 210.
[53] Ot.prp.nr.94 (2008-2009) s. 135.

skyldkrav for å bli ansvarlig for egenandelen på 1.200 kroner – det er tilstrekkelig at uvedkommende har skaffet seg tilgang til sikkerhetsanordningene.

Egenandelen gjelder dermed både der kunden ikke har utvist noen skyld i hele tatt, og der kundens opptreden er uaktsom. Bestemmelsen kommer til anvendelse for eksempel dersom uvedkommende får tilgang til personnummer, BankID-kode og personlig passord til nettbanken.[54] Det vil også gjelde ved såkalt phishing, der kunden for eksempel får en mail som etterspør kortnummer og annen informasjon fra kortet som kan brukes til å gjennomføre transaksjoner.[55] Ved hacking av datasystemer kan kunden vanskelig sies å ha mislyktes i å beskytte sikkerhetsanordningene sine, ettersom det er svært vanskelig å beskytte seg mot hacking.[56]

Etter § 35 tredje ledd første punktum øker kundens egenansvar til hele tapet dersom kunden ved «grov uaktsomhet» har unnlatt å oppfylle pliktene sine etter § 34 første ledd. Se nedenfor i kapittel 2.5 for en nærmere gjennomgang av uaktsomhetsvilkåret og pliktene etter § 34. Her skal det kun påpekes at tredje ledd inneholder et skyldkrav som andre ledd ikke har. Dette gjør også at egenandelen øker til hele tapets størrelse. I andre punktum er det inntatt en beløpsbegrensning for «elektroniske betalingsmidler». Kunder som er utsatt for misbruk av betalingskort eller nettbank hefter derfor bare for inntil 12.000 kroner av tapet. I tredje og fjerde punktum kommer unntak fra dette unntaket. Dersom kunden forsettlig har unnlatt å oppfylle forpliktelsene sine, eller dersom han har opptrådt svikaktig, skal kunden hefte for hele tapet uansett hva slags betalingsinstrument som er brukt.

[54] Krüger, Rettsdata, Finansavtaleloven, note (216).
[55] Grøttjord/Rosén s. 211.
[56] Ot.prp.nr.94 (2008-2009) s. 135.

2.5 Nærmere om forpliktelsene etter finansavtaleloven § 34 første ledd

Finansinstitusjonen har anledning til å holde kunden ansvarlig for hele det økonomiske tapet, eller 12.000 kroner av tapet ved misbruk av elektroniske betalingsmidler, etter § 35 tredje ledd. Forutsetningen er at kunden opptrådte grovt uaktsomt da han unnlot å følge forpliktelsene sine etter § 34 første ledd. Bestemmelsen krever at kunden bruker instrumentet «i samsvar med vilkår for utstedelse og bruk», herunder tar «alle rimelige forholdsregler» for å beskytte sikkerhetsanordningene knyttet til instrumentet. For betalingskort er disse vilkårene standardvilkår i avtalen mellom kunden og institusjonen, og er nøyaktig de samme i de fleste banker.[57] Av standardvilkårene følger for det første at kunden må påse at ingen uvedkommende får tak i kortet, heller ingen som kunden anser som betrodde mennesker. Videre skal koden ikke røpes til noen, og heller ikke skrives ned på en slik måte at andre enn kontohaveren ikke kan forstå hva sifrene gjelder. Et notat som angir koden må aldri oppbevares sammen med kortet.

Kunden skal ta alle «rimelige» forholdsregler for å beskytte sikkerhetsanordningene. Dette tilsier at de tiltak en forbruker skal iverksette for at uvedkommende ikke skal få anledning til å misbruke instrumentet ikke kan være uforholdsmessig tyngende. Videre kan det heller ikke kreves at tiltakene går ut over betalingsinstrumentets anvendbarhet, for eksempel at kunden til enhver tid må ha betalingskortet med seg.[58] Derimot vil det ikke være urimelig å kreve at sikkerhetsanordningene oppbevares adskilt fra betalingsinstrumentet.[59]

I tillegg skal kunden melde fra til institusjonen «uten ugrunnet opphold» dersom han blir oppmerksom på uautorisert bruk av noe slag, eller tap eller tyveri av kortet. Det kreves altså faktisk kunnskap om tap, tyveri eller uautorisert bruk før meldeplikten trer i kraft – det er ikke

[57] Se for eksempel https://www.dnb.no/portalfront/dnb/nedlast/privat/avtaler/kontoavtale-vilkaar-visa-mastercard-E.pdf?popup=true (sist besøkt 28.05.2018), https://www.spv.no/-/media/Files/kort/avtalevilkar/Avtale-om-betalingskort.pdf (sist besøkt 28.05.2018), https://www.nordea.no/Images/57-82383/Cards%20-%20Avtalevilk%C3%A5r%20Nordea%20Bankkort.pdf (sist besøkt 28.05.2018) og https://danskebank.no/nb-no/Privat/Documents/Generelle-vilkaar_Platinum.pdf (sist besøkt 28.05.2018).
[58] Grøttjord/Rosén (2014) s. 205.
[59] l.c.

nok at kunden burde visst at instrumentet var stjålet eller borte. Videre er fristen relativ, slik at det beror på en konkret vurdering hvorvidt kunden har overholdt fristen eller ikke.

Når det gjelder Vipps er spørsmålet om forbrukeren har en slik meldeplikt for å forhindre at Vipps-profilen blir brukt til å gjennomføre uautoriserte transaksjoner. Underrettelsesplikten gjelder tap, tyveri eller uberettiget tilegnelse av «betalingsinstrumentet». Dersom en mobiltelefon med Vipps-profil blir stjålet, vil betalingsinstrumentet komme på avveie sammen med enheten. Dermed må forbrukeren underrette institusjonen dersom enheten kommer på avveie. Forbrukeren kan enten underrette Vipps for å sperre Vipps-profilen eller sin egen bank for å sperre betalingskortet. [60]

[60] www.vipps.no/sporsmal – «Jeg har mistet telefonen min» (sist besøkt 12.03.2018).

3 Uaktsomhetsvilkåret

3.1 Innledning

Grov uaktsomhet fra kundens side har i årtier vært brukt som grunnlag for kundens ansvar for egenandel i EU-retten.[61] I dag følger det av PSD 1 artikkel 59 at dersom forbrukeren har unnlatt å oppfylle sine plikter etter artikkel 56 ved «grov forsømmelse», hefter forbrukeren i utgangspunktet for hele den uautoriserte transaksjonen.[62] Om innholdet i begrepet «grov forsømmelse» uttales det i fortalen til PSD 2 avsnitt 72 at vilkåret må inneholde mer enn den rene uaktsomhet, og at det må være tale om «betydelig grad af skødesløshed». Som eksempel nevner fortalen i samme avsnitt at oppbevaring av sikkerhetsanordninger sammen med betalingsinstrumentet er et eksempel på grov forsømmelse. Dette kapitlet skal gjøre rede for hvordan begrepet er fastlagt i norsk, svensk og dansk rett.

3.2 Innholdet i uaktsomhetsvilkåret

3.2.1 Norge

I norsk rett er direktivet på dette punkt gjennomført ved at kunden må ha opptrådt grovt uaktsomt i forbindelse med forpliktelsene han har etter finansavtaleloven § 34 første ledd. Slik vilkåret er tolket av Høyesterett i erstatningsrettslige tvister, innebærer vilkåret at forpliktelsene i § 34 må være brutt ved at kunden har utvist en atferd som klart avviker fra det en alminnelig fornuftig person ville gjort.[63] En nærmere klarlegging får vi ikke i lovgivningen. Det nærmeste man kommer en drøftelse av vilkåret i for- og etterarbeidene til finansavtaleloven er generelle uttalelser om at det kreves et markert avvik fra vanlig forsvarlig handlemåte.[64] I Rt. 2004 s. 499 kom Høyesterett med retningslinjer til hvordan vilkåret skal

[61] Recommendation 88/590/EEC punkt 4.2.
[62] Pliktene er nøyaktig de samme som i finansavtaleloven § 34 første ledd, som er behandlet ovenfor i kapittel 2.5.
[63] Se blant annet Rt. 2004 s. 1942 avsnitt 38, Rt. 2008 s. 1360 avsnitt 16, HR-2016-1464-A avsnitt 60.
[64] Se for eksempel NOU 1994:19 s. 181 og Ot.prp.nr. 94 (2008-2009) s. 119.

forstås med hensyn til finansavtaleloven § 35 tredje ledd. I denne saken hadde kunden oppbevart betalingskortene sine i en låst koffert i en låst leilighet i Barcelona. Sammen med kortene lå en syvende sans der kodene til kortene var skrevet ned. Kodene var kamuflert ved at sønnenes fødselsdatoer var føyd til foran og etter koden, og foran tallrekken sto sønnenes initialer. Kortene ble stjålet, og det ene kortet ble misbrukt. Banken mente han hadde handlet grovt uaktsomt ved å kamuflere kodene på denne måten.

Om vurderingen av spørsmålet om grov uaktsomhet, uttalte en samlet rett at det «må bero på en samlet bedømmelse av hvor godt koden var kamuflert og hvordan den ved anledningen ble oppbevart.» [65] Høyesteretts flertall på tre dommere mente kunden ikke hadde opptrådt grovt uaktsomt. Flertallet uttalte at «A kan bebreides for ikke å ha kamuflert koden godt nok når han på denne måten valgte å notere den i sin syvende sans», og videre at det var «ubetenksomt av A å la kort og kode bli liggende i kofferten». Når flertallet likevel mente at uaktsomheten ikke var grov, la de avgjørende vekt på at oppbevaringen av kort og kode sammen hadde et «klart midlertidig preg», og at vurderingen hadde blitt en annen hvis oppbevaringen var av permanent karakter.

Høyesterett tillot altså at koden ble oppbevart sammen med betalingskortet, selv om kamufleringen ikke var god nok. I avsnitt 32 bygget en samlet rett på Rt. 1989 s. 1318, der det ble uttalt at oppførselen må «representere 'et markert avvik fra vanlig forsvarlig handlemåte', og at det må dreie seg om 'en opptreden som er sterkt klanderverdig', hvor vedkommende er 'vesentlig mer å klandre enn hvor det er tale om alminnelig uaktsomhet'». Disse uttalelsene viser at det må foretas en konkret helhetsvurdering av forbrukerens handlinger. Videre tyder uttalelsene på at steget fra simpel uaktsomhet opp til grov uaktsomhet er svært langt. Det er dermed en høy terskel som skal overskrides før det blir tale om ansvar på grunn av grov uaktsomhet.

[65] Se kapittel 4.1 for en grundigere analyse av kamuflering av PIN-koder. Poenget her er kun å komme frem til Høyesteretts tolkning av «grov uaktsomhet» i finansavtaleloven § 35 tredje ledd.

3.2.2 Komparativt: uaktsomhetsvilkårets innhold i svensk og dansk rett

Den svenske lagen om obehöriga transaktioner 6 § bruker samme begrep som den norske finansavtaleloven. Rent språklig er de derfor helt like, noe som tilsier at man praktiserer vilkåret likt i norsk og svensk rett. Det følger også av lovens forarbeider at det skal «vara fråga om ett markant avsteg från aktsamhetsnormen» i en «sådan grad att han eller hon inte är ursäktad».[66] Disse uttalelsene stemmer godt overens med hvordan vilkåret er forstått i norsk rett.

Betalingslovens ordlyd om «groft uforsvarlig adfærd» i § 100 stk. 4 nr. 3 avviker ikke stort fra den norske og svenske ordlyden. Språklig sett peker også dette vilkåret på et markert avvik fra den rene uforsvarlige, uaktsomme atferd. Tidligere lovgivning krevde imidlertid «grov uaktsomhed» fra betaleren.[67] Dette tilsier at man har ment å foreta en realitetsendring med tanke på hvordan uaktsomhetsvilkåret skal forstås. I merknadene til endring av den gjeldende betalingsloven, ble det uttalt at med endringen fra «grov uaktsomhed» til «groft uforsvarlig adfærd» var det «tilsiktet en væsentlig skærpelse af ansvarsbetingelsen i forhold til hidtidig praksis i Pengeinstitutankenævnet med hensyn til opbevaring af PIN-koder sammen med kort».[68] Formålet med endringen var altså å øke terskelen for at egenansvaret skulle inntre. Dette tyder på at dansk rett praktiserer «grov forsømmelse» annerledes enn norsk og svensk rett, til tross for målsetningen om rettsenhet i TEU. Det er imidlertid viktig å være oppmerksom på at dette kun gjelder «med hensyn til opbevaring af PIN-koder sammen med kort», slik at hevingen av terskelen i så fall må begrenses til å gjelde i disse tilfellene.[69] I alle andre tilfeller gjelder derfor samme uaktsomhetsterskel som tidligere, og må antas å ha samme innhold som i norsk og svensk rett.

[66] Prop. 2009/10:122 s. 27.
[67] von Eyben (1993) s. 623-624.
[68] Lovforslag nr. L 60, Folketinget 1991-1992.
[69] l.c

4 Analyse av typetilfeller der spørsmålet er om kunden har opptrådt grovt uaktsomt

4.1 Kamuflasje av PIN-koden

4.1.1 Innledning

Mange sliter med hukommelsen eller har mange ulike koder å huske på. For disse fremstår det som praktisk å kamuflere koden, for eksempel ved å legge til sifre foran og/eller bak PIN-koden, eller å bruke koder eller andre tallsystemer. Det er imidlertid knyttet stor risiko til dette, fordi det gir tyver en mulighet til å misbruke kortet og gjennomføre uautoriserte transaksjoner. Dette understrekes av at mange av sakene som kommer inn til Finansklagenemnda gjelder manglende kamuflering eller for dårlig kamuflering av koden.[70] Spørsmålet er om koden kan oppbevares i nærheten av kortet i kamuflert form uten av kunden har opptrådt grovt uaktsomt, og i så fall hvilke minimumskrav som må stilles til kamuflasjen.

4.1.2 Grensen mellom simpel og grov uaktsomhet i norsk rett

I Rt. 2004 s. 499 godtok Høyesteretts flertall kamuflasjen på tross av at kamuflasjen var for dårlig og på tross av at det var ubetenksomt å la kort og kode ligge i kofferten. Denne atferden ble ansett for å være simpel uaktsom, og ikke grovt uaktsom. Dette kan synes å være en mer forbrukervennlig posisjon enn det Finansklagenemnda tidligere har inntatt. Nemnda har tillatt oppbevaring av kort og kode sammen kun dersom kamufleringen er god nok til at andre ikke forstår at det er koden som er notert.[71] Årsaken til at Høyesterett kom til denne konklusjonen ser ut til å være den midlertidige karakteren av oppbevaringen av kort og kode sammen, ettersom Høyesterett lot dette være det avgjørende frifinnende argumentet. Hvis kort og kode

[70] Se https://publisering.finkn.no/keywords/4/AZ0101 (sist besøkt 21.03.2018), der det fremgår at 79 saker gjelder ukamuflert eller dårlig kamuflert kode.
[71] Torvund (2003), sjette avsnitt fra bunnen.

skal oppbevares sammen permanent, kreves derfor en bedre kamuflering enn i tilfellet Høyesterett tok stilling til.

Finansklagenemnda har senere uttalt at det anses som grovt uaktsomt dersom koden blir oppbevart sammen med kortet i ukamuflert form, uansett om man har en sykdom eller tilstand som gjør at man har vanskeligheter med å huske koden.[72] Det er vanskelig å være uenig med nemnda i at en alminnelig fornuftig person aldri ville oppbevart PIN-koden sammen med betalingskortet uten å kamuflere den, og at dette utgjør et markert avvik fra det normale.

Ved enkelte tilfeller har nemnda likevel lagt til grunn en for lav terskel sett opp mot den som er lagt til grunn av Høyesterett. I BKN-2012-541 uttalte nemnda at «ettersom misbrukeren tastet riktig kode på første forsøk, legger flertallet til grunn at koden ikke var kamuflert i tilstrekkelig grad». En tyv vil alltid lete etter mulige kombinasjoner, og noen ganger har tyven flaks. Dette betyr imidlertid ikke at forbrukeren med nødvendighet har kamuflert koden for dårlig, noe nemnda synes å legge til grunn. Det er uheldig å bruke antallet forsøk tyven måtte bruke for å knekke koden for å avgjøre hvor godt kamuflert koden var. Det mest naturlige ville vært å se på selve kamufleringen. Spørsmålet i det følgende blir når kamufleringen i seg selv er så dårlig at den kvalifiserer til grov uaktsomhet.

I Finansklagenemndas avgjørelse i BKN-2015-019 ble et tilfelle som ligner på Rt. 2004 s. 499 vurdert annerledes av nemnda. Betalingskortet ble stjålet fra et feriehus. Det ble også stjålet en sekk med en syvende sans der koden til kortet var skrevet ned. Nemnda mente at denne saken skilte seg fra Rt. 2004 s. 499 på to måter. For det første ved at koden ikke var «forsøkt kamuflert på annen måte enn ved at den var en av fire tallrekker uten tekst», og for det andre fordi «kort og kode [ble] oppbevart nær hverandre på mer varig basis». Her var altså kamufleringen dårlig, slik som i Rt. 2004 s. 499. Oppbevaringen av kort og kode sammen hadde imidlertid en mer permanent karakter, slik at det frifinnende argumentet Høyesterett

[72] Se for eksempel BKN-2014-131.

brukte, ikke kom til anvendelse. Dermed ble konklusjonen at kunden hadde opptrådt grovt uaktsomt.

Fra disse sakene kan det utledes at kamuflasjen bør være omfattende, der tallrekkene som inngår i kamufleringen må inneholde mer enn fire sifre, slik at tallrekkene ikke uten videre kan assosieres med PIN-koder. Videre har det stor betydning hvor midlertidig oppbevaringen av kortet sammen med koden er. Særlig på reise er det derfor anledning til å oppbevare kode og kort sammen i en kort stund, for eksempel i forbindelse med en nært forestående avreise, uten å ha opptrådt grovt uaktsomt.

I BKN-1997-031 hadde kunden fått betalingskortet misbrukt etter å ha kamuflert koden gjennom å bruke navn eller initialer foran et fiktivt telefonnummer. Alle numrene startet med 22 og endte med 00. Nemnda uttalte at kunden «nok har vært uaktsom» fordi det er «godt kjent blant kriminelle» at koder kamufleres på denne måten. Likevel var ikke uaktsomheten grov fordi kunden «tross alt [hadde] gjort et forsøk» på å kamuflere PIN-koden, i tillegg til at banken hadde gitt manglende informasjon om risikoen som var knyttet til denne kamufleringsmåten. Forsøk på å kamuflere koden i et telefonregister er dermed ikke grovt uaktsomt ifølge Finansklagenemnda, selv om det var tydelig at numrene kunne være fiktive.

I RG. 2002 s. 1273 hadde kunden også kamuflert kodene i form av telefonnumre ved å legge til 55 og 22 foran koden, og 00 etter koden. I tillegg var navnet «Eva» skrevet foran koden til Eurocard-kortet og «Victor» foran Visa-kortet. I tråd med tidligere praksis, konkluderte nemnda med at kundens handlemåte ikke var grovt uaktsom. Banken saksøkte imidlertid kunden, og lagmannsretten kom til en annen konklusjon enn nemnda. Det ble uttalt at «nedtegning av koden i en slik situasjon ikke i seg selv [kan] karakteriseres som grovt uaktsom». Likevel var det to forhold som gjorde at kunden hadde opptrådt grovt uaktsomt. For det første «at hun skrev ned begge kortenes PIN-koder på samme papirlapp i en så dårlig kamuflert form som nevnt», og for det andre «at hun oppbevarte lappen i pengeboken sammen med bankkortene, der de ble værende også etter at hun kom tilbake fra sin utenlandsferie».

Lagmannsretten brukte også her oppbevaringens permanente karakter som et skjerpende moment. Dette fremstår dermed som et viktig moment ved uaktsomhetsvurderingen. Videre er det ikke lenger en forsvarlig praksis å kamuflere koden som telefonnummer. Antakeligvis gjelder dette først og fremst når det blir for åpenbart at nummeret er fiktivt. Dersom kamufleringen fremstår som et reelt nummer, er det mindre grunn til å tro at en tyv vil forstå sammenhengen. Videre bør koden være kamuflert i et omfattende telefonregister og ikke skille seg fra andre numre i listen som inneholder koden.[73]

I BKN-2006-080 var koden oppbevart permanent sammen med betalingskortet. Den var kamuflert blant elleve reelle og fiktive telefonnumre og fem fødselsdatoer slik at koden utgjorde annethvert siffer i én av disse tallrekkene. Nemnda uttalte at «[d]ersom listen hadde vært oppbevart et annet sted enn i lommeboken, eksempelvis i vesken, ville tilknytningen ikke vært like åpenbar», slik at oppbevaringsmåten utgjorde et skjerpende moment. Likevel var kamufleringen «relativt god», slik at dette gjorde opp for uforsiktigheten ved å oppbevare koden sammen med kortet. Det ble her lagt vekt på at korrekt PIN-kode først ble tastet på tredje forsøk og at kamufleringen gjorde at det må ha «berodd på noe flaks at misbrukeren har funnet frem til» koden. I motsetning til de tilfellene der nemnda automatisk går ut fra at koden var for dårlig kamuflert siden koden ble tastet riktig på første forsøk, er det uproblematisk å bruke samme type argumentasjon her. Det er et moment under vurderingen av hvor god selve kamuflasjen var, ikke en antydning til at en ukjent kamufleringsmåte var for dårlig.

Basert på denne retts- og nemndspraksisen kan det utledes at en kunde har opptrådt grovt uaktsomt dersom kunden har oppbevart koden sammen med betalingskortet på permanent vis, og koden bare er kamuflert som et telefonnummer som fremstår fiktivt. For at telefonnummeret skal fremstå reelt bør kamufleringen være en del av et omfattende telefonregister og ikke skille seg ut fra de andre numrene i registeret. Dersom oppbevaringen bare har en midlertidig karakter, kan dette imidlertid tale til fordel for kunden dersom kamufleringen ellers er god nok. Hvis kunden oppbevarer kortet sammen med koden

[73] Torvund (2003), siste avsnitt.

permanent, er uaktsomheten derimot ikke grov dersom kamufleringen er tilstrekkelig god, slik at tyven må være heldig for å gjette riktig kode.

4.1.3 Komparativt

Fra dansk praksis skal først nevnes avgjørelsen i 205/2005. Kunden oppbevarte kortet sammen med jakken bak disken i butikken han jobbet i. Sammen med kortet oppbevarte kunden flere papirlapper, der den ene inneholdt et firesifret nummer som tilsvarte kortets PIN-kode. Kortet ble stjålet og misbrukt med riktig PIN-kode. Pengeinstitutankenævnet, som tilsvarer den norske finansklagenemnda, mente at «det må bebrejdes klageren, at pinkoden til kortet var anført på en seddel, der lå i pungen sammen med kortet», men at dette ikke kvalifiserte til «groft uforsvarlig adfærd». Nemnda viste til forarbeidene, som uttalte at det utvidede ansvaret for tapet «kun vil kunne gøres gældende i et fåtal af tilfælde».

I 320/2007 hadde kunden blitt frastjålet lommeboken, der han oppbevarte både betalingskortet og PIN-koden. PIN-koden var skrevet ned på en pappbit, og var ikke forsøkt kamuflert. Nemnda konkluderte med at «det må bebrejdes klageren, at PIN-koden til kortet var anført på et papstykke, der lå i pungen sammen med dankortet», men at dette ikke var nok til å kvalifisere til «groft uforsvarlig adfærd». Disse to sakene er helt i strid med norsk praksis, og den norske nemnda ville i et slikt tilfelle etter all sannsynlighet konkludert med at kunden klart hadde opptrådt grovt uaktsomt. Det er vanskelig å tenke seg tilfeller der kunden har opptrådt grovt uaktsomt dersom disse tilfellene ikke kvalifiserer. Dansk praksis er dermed mer forbrukervennlig enn Finansklagenemnda, og det virker som at unntaket om ansvar ved «groft uforsvarlig adfærd» ikke har noen selvstendig betydning når det gjelder kamuflering av PIN-koder.

4.2 Tyveri fra hotellrom eller annet midlertidig bosted

4.2.1 Grensen mellom simpel og grov uaktsomhet i norsk rett

På reise blir man utsatt for en større risiko for å bli frastjålet betalingskort enn i hjemmet. Ved å bo på hotell eller fremstå som turist vil man bli et sårbart mål for kriminelle. Dette krever også normalt at kunden er mer påpasselig enn i kjente omgivelser. Den følgende analysen av praksis som gjelder tyveri fra hotellrom eller andre midlertidige bosteder tar sikte på å finne grensen mellom simpel og grov uaktsomhet når kunden forlater kortet og dermed mister den fysiske besittelsen over det. I tillegg vil fremstillingen ta opp spørsmålet om det er adgang til å oppbevare koden i nærheten av kortet på et slikt midlertidig bosted.

I BKN-2000-050 var kunden i Miami og bodde på sovesal på hostell. Der ble han kjent med to utlendinger som tilbød ham å oppbevare kortene i en oppbevaringsboks som kun den ene utlendingen hadde nøkkel til, og på ett tidspunkt ble kortene stjålet og misbrukt. Spørsmålet var om kunden hadde opptrådt grovt uaktsomt ved å legge kortet i en safe han ikke hadde tilgang til. Nemnda uttalte at kunden hadde opptrådt «uaktsomt [...] ved å plassere kortene i boksen». På den andre siden la nemnda vekt på at det ikke forelå et «praktisk gjennomførbart alternativ som fremstod som sikrere når han for eksempel skulle ut og bade». Han var derfor kommet i et dilemma og valgte en «løsning som subjektivt fremstod som fornuftig og rimelig sikker». Konklusjonen fra nemnda ble dermed at kundens uaktsomhet ikke ble ansett som grov.

I BKN-2006-084 var kunden på ferie i Jerusalem og oppbevarte kortet i en Filofax på hotellrommet mens han selv var ute. Kortet ble stjålet og misbrukt. Om uaktsomhetsvurderingen uttalte nemnda at det normalt ikke kan «anses grovt uaktsomt at man på reise i utlandet [...] legger enkelte verdisaker igjen på hotellrommet når man ferdes ute, selv om verdisakene da ideelt sett bør oppbevares i safe eller lignende». I dette tilfellet hadde kunden også oppbevart kortet i en Filofax i en koffert og ikke «fremme åpenlyst på hotellrommet». Dermed ble konklusjonen at kunden ikke hadde opptrådt grovt uaktsomt. Tatt

i betraktning at nemnda ikke uttalte seg om simpel uaktsomhet, virker det som at denne opptredenen ble bedømt som normal aktsom adferd. Det kan innvendes at dersom verdisakene «ideelt sett bør oppbevares i safe eller lignende», vil adferden i dette tilfellet være et avvik fra hvordan en alminnelig forstandig person ville opptrådt. Forbrukeren i denne saken burde derfor vært ansett for å ha opptrådt uaktsomt.

I BKN-2010-062 fikk kunden frastjålet betalingskortet sitt fra et hotellrom i København. Kortet lå i en lommebok på nattbordet. På den andre siden av sengen, i en koffert, var koden nedskrevet i ukamuflert form. Sammen med koden lå det også 250 sider med tall. Nemnda uttalte at de la vekt på at «koden var nedtegnet i ukamuflert form og oppbevart på et hotellrom som må anses å være et mindre trygt oppbevaringssted enn et privat hjem». Videre mente nemnda at «kortholder med små anstrengelser kunne ha gjort det vanskeligere for uvedkommende å få tilgang til både kort og kode, for eksempel ved å kamuflere koden eller ta med seg kortet da han skulle spise». Konklusjonen ble derfor at kunden hadde opptrådt grovt uaktsomt.

Denne praksisen viser at det ikke i seg selv er grovt uaktsomt å legge igjen betalingskortet på hotellrommet dersom man har forsøkt å gjemme det eller låse det ned. I de tilfellene der man må oppgi den fysiske besittelsen over kortet uten at det eksisterer andre gjennomførbare måter å forhindre tyveri på, skal det mye til for at kunden har opptrådt grovt uaktsomt. Dette fremgår av BKN-2000-050, der bading var årsaken til at han ikke hadde besittelse over betalingskortet; man skulle jo anta at i valget mellom å bade og å beskytte betalingskortet sitt mot misbruk, ville sistnevnte utvilsomt ha størst prioritet. Dersom kortet ligger lett tilgjengelig på hotellrommet, har man derimot handlet uaktsomt. Hvis koden i tillegg blir oppbevart på rommet, og kunden ved enkle grep kunne redusert risikoen for tyveri og misbruk, vil kundens opptreden kvalifisere til grov uaktsomhet.

4.2.2 Komparativt

I 2002-8212 avgjorde den svenske nemnda spørsmålet om en kunde hadde opptrådt grovt uaktsomt der et betalingskort hadde blitt stjålet fra en hotelleilighet mens korteieren var ute av

leiligheten. Samtidig som tyveriet pågikk, befant korteierens datter seg i naborommet uten å merke noe. Utgangspunktet for uaktsomhetsdrøftelsen var forarbeidenes veiledende uttalelser om at det foreligger grov uaktsomhet når kortet blir etterlatt et sted «som inte stått under uppsikt».[74] Avgjørende ble at «[d]et hade [...] varit lätt för C att förhindra stölden genom att ta med sig kortet, låsa dörren eller förvara kortet på ett sådant sätt att hennes dotter hade uppsikt över det. Nemnda mente dermed at kunden ikke hadde hatt kortet under tilstrekkelig oppsyn, og derfor opptrådt grovt uaktsomt. Dette er et argumentasjonsmønster vi kan kjenne igjen fra norsk praksis, jf. ovenfor i kapittel 4.2.1. Enkle alternative handlinger, som å ta med seg kortet eller å oppbevare kortet på en annen måte, for eksempel mindre tilgjengelig, ble unnlatt. Her skal det nok likevel noe mindre til enn i norsk rett for å ha opptrådt grovt uaktsomt. Som vist i BKN-2006-084, er det ikke grovt uaktsomt å la kortet ligge på rommet uten tilsyn, mens det i denne saken ble brukt som skjerpende moment i uaktsomhetsvurderingen.

I 2001-4153 var kunden på ishockeyskole, og skulle sove i en gang med sju andre mennesker. Han oppbevarte betalingskortet i shortslommen på en benk i nærheten av der han sov. Kortet ble stjålet og misbrukt i løpet av natten. I uaktsomhetsvurderingen viste nemnda til en tidligere plenumssak der et betalingskort ble stjålet fra en entré i en ulåst bolig. I den saken mente nemnda at det ikke var grovt uaktsomt å oppbevare kortet på denne måten. I den foreliggende saken parallelltolket nemnda faktum med plenumsavgjørelsen, og mente at kunden hadde «förvarat kortet i sin omedelbara närhet när han sov i det rum som tjänade som hans tillfälliga bostad under ett hockeyläger». Det forelå heller ingen «särskilda omständigheter som bort föranleda N att iaktta större försiktighet eller vidta ytterligare försiktighetsåtgärder». Kunden hadde dermed ikke opptrådt grovt uaktsomt. Det er oppsiktsvekkende at nemnda her sidestilte permanent bolig med en ishockeyhall, og at det ifølge nemnda ikke forelå omstendigheter som foranlediget større forsiktighet. Det er nettopp den midlertidige karakteren som ofte gjør oppbevaringen mindre sikker, og som stiller større krav til hvordan forbrukere oppbevarer betalingskort.[75]

[74] Prop. 1976/77:123 s. 191.
[75] Se BKN-2010-062, der nemnda slo fast at «hotellrom som må anses å være et mindre trygt oppbevaringssted enn et privat hjem».

Hovrätten kom til en annen konklusjon i en lignende sak i T 72/92.[76] Kunden var på togreise, og sov i en sovekupé med flere ukjente personer. Betalingskortet lå i en jakkelomme ved siden av sengen, og ble stjålet i løpet av natten. Hovrätten mente at det var enkelt å forhindre tyveriet ved å oppbevare kortet i en plastlomme rundt halsen eller under hodeputen, og han hadde derfor ikke kortet under tilstrekkelig oppsikt. Retten mente derfor at kunden hadde opptrådt grovt uaktsomt. Hovrätten anerkjente at det midlertidige bostedet var et mindre sikkert sted med tanke på oppbevaring av kort, i motsetning til Reklamationsnemnden. Denne praksisen fremstår likevel som noe strengere enn den norske forståelsen av uaktsomhetsvilkåret, slik denne er utpenslet i kapittel 4.2.1. Etter svensk rett må kunden holde betalingskortet under oppsyn til enhver tid for ikke å bli ansett for å ha opptrådt grovt uaktsomt. I norsk rett er det nødvendig at betalingskortet er lett tilgjengelig på det midlertidige bostedet for å konstatere grov uaktsomhet, men det er akseptabelt å forlate kortet. En likhet er at man etter både norsk og svensk rett alltid vurderer hvor enkelt det var å forhindre tyveriet og misbruket.

4.3 Tyveri fra privat hjem

4.3.1 Grensen mellom simpel og grov uaktsomhet i norsk rett

Ens eget private hjem blir gjerne ansett som en privatsfære der man skal kunne forvente å oppholde seg i fred og uten at uvedkommende skaffer seg adgang. Det foreligger dermed ikke en like stor oppfordring til å iverksette preventive tiltak for å minske eller eliminere risikoen for tyveri og misbruk av betalingsinstrumenter sammenlignet med når man reiser. Dette tilsier i utgangspunktet at det skal mer til for å ha opptrådt grovt uaktsomt når tyveriet skjer fra eget hjem enn når det skjer på reise.

I BKN-2003-049 ble det gjort innbrudd i kundens hjem ved at tyven tok seg inn gjennom et kjellervindu. Betalingskortet ble oppbevart i lommeboken, og koden ble oppbevart ukamuflert i en kommode et annet sted i huset. Banken mente det var grovt uaktsomt å oppbevare koden i

[76] Gjengitt i Bergström (2010) s. 20 (studentavhandling).

nærheten av betalingskortet. Nemnda uttalte på sin side at kunden «må ha anledning til å oppbevare PIN-koden et eller annet sted, mest nærliggende i sitt private hjem». Dette fremstår som velgrunnet, nettopp fordi hjemmet er det stedet man minst vil regne med tyveri sammenlignet med andre steder.

4.3.2 Komparativt

Det kan tenkes at visse tiltak bør gjøres for å unngå grov uaktsomhet selv om hjemmet er et sted man forventer å være i fred fra tyver. Det er for eksempel ikke heldig dersom tyven kan ta seg inn en ulåst ytterdør, og kortet er det første tyven får øye på etter å ha gått inn. Dette finnes det ingen praksis på i norsk rett, men både svensk og dansk nemndspraksis har avgjort disse spørsmålene.

I 1999-1705 behandlet den svenske nemnda i plenum en sak der et kort ble stjålet fra en leilighet på natten. Døren til leiligheten sto ulåst, men døren til selve bygningskomplekset var låst. Betalingskortet var lett tilgjengelig i en jakkelomme i leilighetens entré. Nemnda tok utgangspunkt i en presumsjon for «att grov oaktsamhet normalt inte får anses föreligga, om kontokortet förloras när det förvaras i bostaden». Deretter uttalte flertallet at den eneste omstendigheten som avvek fra en normal aktsom opptreden var den ulåste ytterdøren, og dermed forelå ingen omstendigheter «som krävs för att grov oaktsamhet skall anses föreligga».

Ifølge den svenske nemnda er det altså uaktsomt, men ikke grovt uaktsomt, å oppbevare kortet i en ulåst leilighet med kortet relativt lett tilgjengelig. Denne løsningen er ikke gitt, med tanke på de strenge kravene forarbeidene stiller til kortholderens kontroll med betalingskortet.[77] Selv om det neppe kan kreves at kortet holdes under oppsyn til enhver tid i eget hjem, bør det nok kreves at kortholderen holder døren låst på nattestid. Med tanke på avstanden fra uaktsom opptreden til grovt uaktsom opptreden, var det likevel forsvarlig å konkludere med at denne atferden kun er uaktsom.

[77] Se kapittel 4.2.2.

Den danske nemnda tok stilling til et tilsvarende spørsmål i 333/2000. Kunden hadde forlatt leiligheten uten å låse døren, og ble utsatt for tyveri og misbruk av betalingskort. Nemnda uttalte at «[s]elv om det kan bebrejdes klageren, at han forlod lejligheden uden at låse denne [...] finder vi det [...] betænkeligt at fastslå, at klagerens adfærd i det foreliggende tilfælde var groft uforsvarlig». Denne avgjørelsen gir altså uttrykk for at det er uaktsomt ikke å låse leiligheten, men ikke så uaktsomt at det krysser terskelen for grovt uforsvarlig adferd. Dermed er dansk rett på linje med svensk rett. Med tanke på at norsk rett er noe mer forbrukervennlig enn svensk rett når det gjelder tyveri fra midlertidig bosted, vil den norske nemnda antakeligvis ikke bedømme tilfellene som gjelder permanent bosted noe strengere enn svensk og dansk rett.

I samme sak avgjorde nemnda også om kunden hadde opptrådt grovt uforsvarlig ved at han hadde skrevet ned PIN-koden, og oppbevart denne i leiligheten. Koden var kamuflert som en del av et fiktivt regnskap, og betalingskortet ble for anledningen oppbevart sammen med regnskapet. Nemnda uttalte at «det kan bebrejdes klageren, at han [...] efterlod dankortet samt PIN-koden, der var nedskrevet», men at dette ikke var grovt uforsvarlig adferd.

I 14/2002 lå betalingskortet til kunden sammen med sjekkheftet hans, mens koden ble oppbevart ukamuflert i en brevordner. Om uaktsomhetsspørsmålet uttalte nemnda at det faktum at klageren «opbevarede såvel hævekortet som den tilhørende PIN-kode på sin bopæl kan ikke i sig selv betegnes som groft uforsvarlig adfærd». Her, som under kamufleringstilfellene, virker det som at det utvidede ansvaret ved grovt uforsvarlig adferd ikke har noen praktisk betydning i dansk rett når kunden får medhold i de sakene som er nevnt her. Det er usannsynlig at den norske nemnda vil følge samme terskel som Pengeinstitutankenævnet på dette spørsmålet. Som vist under kapitlene 4.1 og 4.2, vil det utvidede ansvaret inntre dersom kunden oppbevarer kort og kode sammen på permanent basis. Det er liten grunn til å anta at nemnda vil fravike dette utgangspunktet selv om oppbevaringen skjer i kundens eget hjem. I tillegg gjelder standardvilkårene i rammeavtalen mellom kunden og banken også i eget hjem. Dette støttes av Finansklagenemndas noe forsiktige uttalelse i BKN-2003-049, der det heter at kunden «må ha anledning til å oppbevare PIN-koden et eller annet sted, mest nærliggende i sitt private hjem». Dette er ikke en uttalelse

som fritar kunden fra pliktene, men som tillater at koden blir oppbevart et sted så lenge det skjer i samsvar med disse pliktene.

4.4 Tyveri fra bil

4.4.1 Grensen mellom simpel og grov uaktsomhet i norsk rett

Det er vanlig å etterlate betalingskortet sitt i bilen, for eksempel når man gjør ærender som ikke krever bruk av kort. Særlig gjelder dette i tilfeller der kunden er borte fra bilen kun for en kort periode. I BKN-1994-061 hadde kunden parkert bilen på en offentlig parkeringsplass i Spania, omkring 200 meter fra stranden han oppholdt seg på. Betalingskortet oppbevarte han i bilen. I løpet av tiden han var på stranden, ble det gjort innbrudd i bilen, og kortet ble stjålet og misbrukt med signatur. Spørsmålet var om kunden hadde opptrådt grovt uaktsomt ved å forlate kortet i bilen. Nemnda uttalte her at kunden hadde opptrådt uaktsomt ved å etterlate sitt Visakort i bilen, særlig fordi han befant seg på et sted «hvor faren for innbrudd/tyverier må anses allment kjent». Sett i lys av bankens manglende informasjon om at betalingskort kunne bli misbrukt relativt enkelt, og at brukerstedenes kontroll av kundenes underskrift kunne være mangelfull, var uaktsomheten likevel ikke grov.

Nemndas vurdering i dette tilfellet kan synes å være noe streng. Det er vanskelig å se hvilket praktisk alternativ kunden hadde mulighet til å foreta seg i denne situasjonen. Dersom han hadde tatt kortet med seg på stranden, ville han vært utsatt for tyveri i en mye større grad enn ved å legge kortet igjen i bilen. Det virker også strengt å kreve at han burde latt kortet ligge igjen på hotellrommet eller i leiligheten. Som vist tidligere i kapittel 4.2.1, vil man etter nemndas vurdering raskt ha opptrådt like uaktsomt dersom man oppbevarer kortet tilgjengelig på et hotellrom. I tillegg er poenget med betalingskort å ha penger tilgjengelig på en enklere måte enn kontanter. Det må dermed være anledning til å ta kortet med seg selv om kunden skal gjøre aktiviteter som gjør ham mer sårbar for tyveri enn normalt.

I BKN-2006-015 hadde kunden lagt betalingskortet igjen i bilen sammen med andre verdisaker da hun og kjæresten skulle besøke en fornøyelsespark. Mens de var i parken ble det gjort innbrudd i bilen, og et annet betalingskort med samme kode ble stjålet og misbrukt. Banken mente at koden må ha blitt oppbevart sammen med kortet. Omtrent halvannen time før misbruket skjedde, hadde kunden imidlertid brukt kortet i en minibank på et kjøpesenter, der det befant seg mye folk. Nemndas flertall la vekt på at det «gikk ganske kort tid fra kortholders uttak med Visakortet til hennes Mastercard ble misbrukt» og at «det selv fra relativt langt hold kan være mulig å avdekke koden som tastes». Dermed var det ikke sannsynlighetsovervekt for at koden og kortet ble oppbevart sammen, og kunden hadde dermed ikke opptrådt grovt uaktsomt.

Nemnda har tradisjonelt operert med en presumsjon for at koden har vært oppbevart sammen med kortet, og dermed opptrådt grovt uaktsomt, dersom gjerningspersonen har brukt PIN-koden til å misbruke kortet. Dette følger blant annet av BKN-2017-035. Der fastslo nemnda at «[n]år "kikk over skulderen" er lite sannsynlig, og det heller ikke er andre individuelle omstendigheter som kan forklare at uvedkommende har fått kjennskap til koden, har nemnda i sin praksis lagt til grunn at koden må ha vært oppbevart sammen med kortet i åpen eller dårlig kamuflert form».[78] I vår sak virker det som at nemnda gikk bort fra denne presumsjonen; PIN-koden ble brukt, og muligheten til å fange opp koden «fra relativt langt hold» er noe annet enn «kikk over skulderen». En slik innfallsvinkel gjør at nemnda kan gjøre en bedre helhetsvurdering av hendelsesforløpet. I stedet for kun å vurdere hvorvidt PIN-koden er brukt, kan nemnda også vurdere tiden som er gått fra siste bruk av betalingskortet frem til misbruket skjedde. Jo nærmere misbruket er den forrige bruken av kortet i tid, jo mer sannsynlig vil det være at noen har fanget opp koden.

4.4.2 Komparativt

I 1999-2533 behandlet den svenske nemnda i plenum en sak tilsvarende den i BKN-2006-015. Betalingskortet ble lagt igjen i bilen mens kunden var borte i ti minutter for å hente sønnen sin

[78] Se også BKN-2017-001, BKN-2016-452, BKN-2016-093 og BKN-2015-321, der Finansklagenemnda uttaler det samme. Tilsvarende formuleringer er brukt i BKN-2001-017 og BKN-2001-052.

i barnehagen. I løpet av disse minuttene ble det gjort innbrudd i kundens bil, og kortet ble misbrukt med kode. Nemnda la til grunn «att det normalt får anses grovt oaktsamt att lämna kvar kontokortet i en bil som inte stått under uppsikt», fordi det er lett å bryte seg inn i biler. Det er dermed en presumsjon for grov uaktsomhet dersom man forlater betalingskortet i bilen når bilen ikke er under oppsyn. I den konkrete saken konkluderte nemnda med grov uaktsomhet.

Basert på de tre sakene som hittil er nevnt, kan det utledes to observasjoner. For det første fører svensk rett en mye strengere linje enn norsk rett. Selv om det også i norsk nemndspraksis anses uaktsomt å forlate kortet i bilen, skal det mer til for å nå opp til terskelen for grov uaktsomhet enn i svensk praksis. For det andre kan det bemerkes at i norsk rett beror uaktsomhetsvurderingen i større grad på hvordan en tyv har blitt kjent med koden, mens man i svensk rett fokuserer mer på hvor uaktsom selve handlingen å forlate kortet i bilen er.

Den danske nemnda har avsagt tre avgjørelser av interesse. I 386/1997 hadde kunden oppbevart betalingskortet i lommeboken sin, som var plassert i hanskerommet på bilen. Bilen var ulåst, og i lommeboken lå også PIN-koden, kamuflert som et telefonnummer. Nemnda uttalte at kombinasjonen av å etterlate «sin pung indeholdende hævekortet og den tilhørende pinkode i handskerummet i sin uaflåste bil», kvalifiserte til grovt uforsvarlig atferd.

I 685/1992 ble betalingskortet oppbevart i kundens veske i bilen hennes, som var låst. Koden lå også i vesken, i ukamuflert form. Nemnda uttalte at «det kan bebrejdes klageren, at hun opbevarede kort og PIN-kode sammen i sin pung», men at det likevel ikke var tale om en atferd som var grovt uforsvarlig. Denne konklusjonen er i tråd med den forståelsen av uaktsomhetsvilkåret som Pengeinstitutankenævnet har anvendt i andre tilfeller. På samme måte har nemnda lagt seg på en linje som er mer forbrukervennlig enn den norske og svenske nemnda. Den eneste formildende omstendighet i denne saken var at kunden hadde låst bilen, og det virker som at dette momentet er det avgjørende momentet for konklusjonen i uaktsomhetsvurderingen.

I 420/1991 hadde kunden nettopp fått betalingskortet og koden i bankens filial. Både kortet og koden, i ukamuflert form, lå i hanskerommet på bilen, som var låst. Også her kom nemnda til at kunden ikke hadde opptrådt grovt uforsvarlig, og det ble heller ikke nevnt noe om at kunden hadde utvist simpel uaktsomhet.

Etter disse sakene virker det som at den danske nemnda har størst fokus på hvorvidt bilen var låst eller ikke, altså hvor tilgjengelig kortet var. Dersom tyven må bryte seg inn i bilen, skal det mye til for å konstatere grovt uforsvarlig adferd. Dette er i tråd med det nemnda har uttalt om oppbevaring av kort og kode sammen, som vist under kapittel 4.1.3. Det er dermed et stort gap mellom dansk og svensk praktisering av vilkåret i disse tilfellene, der dansk rett er klart mer forbrukervennlig. Norsk praksis ligger i midten, og fremholder at det er uaktsomt å forlate betalingskortet i bil, men at det må mer til enn dette for å konstatere grov uaktsomhet.

4.5 Lekkasje av PIN-koden

4.5.1 Innledning

Det følger av standardvilkårene i rammeavtalen mellom forbrukeren og banken at koden ikke skal røpes til andre personer.[79] Det er uttrykkelig slått fast at dette også gjelder politiet og representanter fra banken. Dersom forbrukeren likevel røper koden overfor uvedkommende, enten ved å si det direkte til den uvedkommende, eller ved at den uvedkommende overhører at koden blir røpt, har kunden dermed brutt vilkårene for bruk av betalingskortet etter finansavtaleloven § 34 første ledd. Spørsmålet i det følgende er når et slikt pliktbrudd utgjør grov uaktsomhet fra kundens side.

[79] Se for eksempel https://www.dnb.no/portalfront/dnb/nedlast/privat/avtaler/kontoavtale-vilkaar-visa-mastercard-E.pdf?popup=true pkt. 21 (sist besøkt 28.05.2018), https://www.spv.no/-/media/Files/kort/avtalevilkar/Avtale-om-betalingskort.pdf pkt. 7 (sist besøkt 28.05.2018), https://www.nordea.no/Images/57-82383/Cards%20-%20Avtalevilk%C3%A5r%20Nordea%20Bankkort.pdf pkt. 7 (sist besøkt 28.05.2018) og https://danskebank.no/nb-no/Privat/Documents/Generelle-vilkaar_Platinum.pdf pkt. 7 (sist besøkt 28.05.2018).

4.5.2 Grensen mellom simpel og grov uaktsomhet i norsk rett

I BKN-2004-116 var kunden på ferie i Praha da han ble spurt av en ukjent person om å ta et fotografi av vedkommende. Etter at han hadde tatt bildene, ble kunden møtt av to menn som utga seg for å være politi. Disse hevdet at det var ulovlig å fotografere på stedet, og ba om kundens bankkort som legitimasjon. I tillegg spurte de om koden til kortet. Kunden oppga koden, og de angivelige politimennene tastet koden inn på et instrument de hadde med seg. Deretter tok de kortet uten at kunden oppdaget det, og misbrukte kortet. Banken mente at kunden hadde opptrådt grovt uaktsomt ved å røpe koden til falske politimenn, selv om de fremsto som ekte politibetjenter.

Finansklagenemnda pekte på to formildende forhold i saken. For det første var kunden i en «svært presset situasjon», slik at det var naturlig at «han ønsket å medvirke best mulig» for å kunne komme seg ut av situasjonen. For det andre skjedde hendelsen i utlandet, slik at «politiets myndighet og praksis ikke var kjent for kortholder». Dermed var det forståelig at han etterkom det han trodde var politiets ordre, for å unngå å gjøre situasjonen mer ubehagelig enn nødvendig. Nemnda konkluderte derfor med at «kortholder nok kan bebreides for at han oppga koden», men at uaktsomheten ikke var grov.

Nemnda fremstår meget forbrukervennlig i denne saken sammenlignet med hvordan den har konkludert i andre typetilfeller.[80] Nemndas tilnærming kan imidlertid ha gode grunner for seg. Én ting er at nemnda valgte å avgjøre saken ut fra hvordan situasjonen fremsto for kunden. Det er likevel også enkelt å tenke seg til mulige konsekvenser dersom han hadde nektet å oppgi koden. Dette var en situasjon der det eneste reelle valget kunden hadde, var å oppgi koden frivillig eller å oppgi den etter å ha blitt utsatt for trusler eller vold. Sistnevnte tilfelle ville åpenbart ikke vært en grovt uaktsom opptreden fra kundens side, og en naturlig konklusjon er dermed at heller ikke en frivillig lekkasje av koden var grovt uaktsomt i det konkrete tilfellet.

[80] Se for eksempel kapittel 4.1, som er nært beslektet med lekkasje av PIN-koden.

I BKN-2004-077 ble kunden oppringt av en person som utga seg for å representere banken. Denne personen opplyste at han behøvde PIN-koden for å klargjøre det nye betalingskortet til kunden, som fortsatt ikke var ankommet. Kunden oppga koden, og kortet ble stjålet før det nådde frem til kunden, antakeligvis av samme person som ringte henne. Nemndas flertall konkluderte med at kunden ikke hadde opptrådt grovt uaktsomt ved å oppgi koden. Ifølge flertallet var det fire formildende forhold som gjorde at kunden ikke hadde vært grovt uaktsom. For det første var «kortholder [...] uforberedt på oppringningen», og for det andre fremsto det ikke som «helt upåregnelig at hun skulle bli kontaktet» i forbindelse med fornyingen av kortet. For det tredje var det ikke «advart mot den aktuelle fremgangsmåte i kortvilkårene eller i bankens informasjonsmateriale». For det fjerde var det tale om en «meget utspekulert metode».

Det kan reises innvendinger til enkelte av flertallets vurderinger. Det er oppsiktsvekkende at det var formildende både at kunden var uforberedt, og at det var påregnelig å bli kontaktet av banken i forbindelse med utstedelsen av nytt kort. Det virker som at flertallet mener at telefonsamtalen var både upåregnelig og påregnelig for kunden på én og samme tid. I tillegg vil enhver telefonoppringning der man blir bedt om å oppgi PIN-koden komme helt uforvarende på kunden, og det følger eksplisitt av vilkårene i rammeavtalen at ingen fra banken skal få kjennskap til koden. Likevel er det som nevnt i kapittel 3.1 et stort sprang fra den rene uaktsomhet og opp til grov uaktsomhet. Det faktum at banken ikke hadde advart mot denne metoden, i tillegg til at det var tale om en utspekulert metode, fremstår som forsvarlige argumenter for at kundens opptreden ikke nådde opp til terskelen for grov uaktsomhet.

I BKN-2003-060 hadde kunden oppgitt koden til mobiltelefonen sin til barnebarnet sitt, slik at barnebarnet kunne bruke mobiltelefonen. Koden var den samme som til betalingskortet, noe barnebarnet fant ut av. Kortet ble deretter misbrukt av barnebarnet. Nemnda uttalte at hvis man bruker samme kode som betalingskortets kode på andre systemer «må kortholder utviste forsiktighet med å gjøre koden kjent når den brukes i andre sammenhenger». Dette har sammenheng med at det vil være naturlig for en person som uberettiget har tilegnet seg et kort å forsøke med koder til andre systemer dersom disse er kjent. Med dette som grunnlag, mente nemnda at «kortholder kan bebreides for at hun oppga koden til mobiltelefonen». I skjerpende

retning ble det lagt vekt på at kunden var «kjent med at [barnebarnet] hadde rusproblemer og et medfølgende behov for penger», og at barnebarnet ofte oppholdt seg hos henne. Flertallet mente imidlertid at uaktsomheten ikke var grov. Kunden hadde gitt koden til barnebarnet muntlig «ved en enkelt anledning», slik at det ikke var «lett å tenke seg at han både skulle lære seg koden og koble denne koden sammen med betalingskortet, som han et par måneder senere skaffet seg tilgang til». Tidsforløpet fremsto altså som upåregnelig for kunden, og hun hadde dermed ikke utvist grov uaktsomhet.

Sett i lys av den høye terskelen Høyesterett har oppstilt for å nå opp til grov uaktsomhet, fremstår konklusjonen i BKN-2003-060 som riktig. Selv om kunden kunne bebreides for å ha oppgitt koden til telefonen når denne var den samme som til betalingskortet, må uaktsomheten antas å være i nedre sjikt. Det er vanskelig å regne med at den som får koden klarer å tenke seg til at koden også kan brukes på betalingskortet.

I BKN-2016-496 hadde kunden oppgitt koden til betalingskortet til barnebarnet. Deretter ble kortet stjålet og misbrukt av samme barnebarn. Nemnda mente dette utgjorde et forsettlig brudd på pliktene etter finansavtaleloven § 34. Dette er naturlig, ettersom vilkårene klart slår fast at koden ikke skal røpes til noen andre.

4.5.3 Komparativt

Avgjørelsen i BKN-2016-496 står imidlertid i sterk kontrast til den danske nemndas avgjørelse i 78/2006. Her hadde kunden røpet koden til kjæresten sin. Dette ble overhørt av en tredjeperson som kunden visste var til stede. Nemnda uttalte at det faktum at uvedkommende «fik mulighed for at overhøre klageren oplyse sin kode til dankortet til kæresten [...] kan ikke betegnes som groft uforsvarlig adfærd». Dette gjaldt «selv om klageren havde givet T adgang til sin bopæl, uanset om hun måtte have kendskab til T's kriminelle baggrund».

Den danske nemnda var i denne saken klart mer forbrukervennlig enn den norske nemnda; der Finansklagenemnda konstaterer forsett, mener Pengeinstitutankenævnet at det ikke foreligger grovt uforsvarlig atferd, selv om sakene er svært like. Finansklagenemnda la i BKN-2003-060 vekt på at kunden visste at barnebarnet hadde rusproblemer og at hun likevel ga ham adgang til boligen der hun oppbevarte kortet. Den danske nemnda avfeide imidlertid lignende argumenter i 78/2006 som irrelevante argumenter i uaktsomhetsvurderingen. Igjen fremstår det som at uaktsomhetsvilkåret i dansk rett ikke har noen praktisk betydning når slike grove forhold får passere. Det er vanskelig å tenke seg klarere brudd på plikten til å beskytte betalingsinstrumentets sikkerhetsanordninger etter PSD 1 artikkel 56 nr. 2.

4.6 Bruk av mobiltelefon eller nettbrett til å gjennomføre uautoriserte betalingstransaksjoner

4.6.1 Innledning

Vipps fungerer slik at kunden laster ned en applikasjon til sin mobiltelefon eller nettbrett. Deretter fyller kunden inn mobilnummer, kortinformasjon og kontoinformasjon.[81] Når dette er på plass, er applikasjonen klar til bruk, slik at enheten kan brukes til å autorisere betalingstransaksjoner. Dermed blir det også aktuelt å bruke mobile enheter til å gjennomføre uautoriserte transaksjoner. Dette er et stadig økende problem ettersom andelen eldre og dermed sårbare mennesker som bruker Vipps øker.[82]

Også yngre vil imidlertid være utsatt for risiko for misbruk, ettersom det er mange ulike måter å bruke Vipps til å gjennomføre uautoriserte transaksjoner på. For det første er det mulig å benytte et hvilket som helst kortnummer for å opprette konto hos Vipps, som deretter kan brukes til å tappe den tilhørende kontoen for penger.[83] For det andre kan misbruk skje ved at kunden låner bort enheten til uvedkommende, for eksempel til å ta en telefonsamtale eller spille musikk i sosiale sammenhenger. For det tredje kan selve enheten bli stjålet. I endel

[81] www.vipps.no/sporsmal (sist besøkt 08.03.2018).
[82] https://dnbfeed.no/privatokonomi/bestemor-og-bestefar-a-laste-ned-vipps/ (sist besøkt 13.03.2018).
[83] Se blant annet https://www.ht.no/nyheter/2016/02/18/Ble-svindlet-for-5.000-kroner-p%C3%A5-Vipps-uten-%C3%A5-ha-appen-12173934.ece (sist besøkt 08.03.2018).

tilfeller har ikke eieren av enheten sikret den med passord eller andre sikkerhetsanordninger. En slik sikkerhetsanordning har ofte heller ikke noen maksgrense for antall mislykkede forsøk før enheten blir sperret slik et betalingskort har. Har uvedkommende først fått tilgang til mobiltelefonen, er det enkelt å få tilgang til Vipps ettersom PIN-koden kan tilbakestilles ved å skrive inn en del av kortnummeret profilen er knyttet til.[84] Mange har i dag også erstattet den ordinære lommeboken med kombinert smarttelefondeksel og kortholder, slik at betalingskort og mobiltelefon i mange tilfeller oppbevares sammen.

Spørsmålet i det følgende er hvordan reglene om uautoriserte betalingstransaksjoner skal forstås når det gjelder misbruk av Vipps.

4.6.2 Overlatelse av instrumentet til andre

Det følger av standardvilkårene i rammeavtalen for bruk av betalingskort at kortet ikke skal «overlates til [...] andre».[85] Hvis forbrukeren gir kortet sitt frivillig til en annen person, og kortet deretter blir misbrukt, vil forbrukerens opptreden mest sannsynlig bli ansett som grovt uaktsom.[86] Spørsmålet er om det samme gjelder hvis overlatelse av mobil enhet fører til misbruk.

Ifølge punkt 6.2 i bruksvilkårene til Vipps er det ikke anledning til å «overlate tilgang til [forbrukerens] Vipps-applikasjon [...] til andre».[87] Videre er det «[forbrukerens] ansvar å påse at andre ikke får tilgang til [forbrukerens] Vipps-applikasjon». Vilkårene er dermed noenlunde de samme som for andre betalingsinstrumenter. I realiteten er det heller ikke noen forskjell mellom Vipps og et betalingskort. Hensynet til likhet og konsekvens i lovgivningen

[84] «Xhabir», saksbehandler i Vipps by DnB (e-postkorrespondanse 25. januar 2018).
[85] Se for https://www.spv.no/-/media/Files/kort/avtalevilkar/Avtale-om-betalingskort.pdf pkt. 7 (sist besøkt 28.05.2018), https://www.nordea.no/Images/57-82383/Cards%20-%20Avtalevilk%C3%A5r%20Nordea%20Bankkort.pdf pkt. 7 (sist besøkt 28.05.2018) og https://danskebank.no/nb-no/Privat/Documents/Generelle-vilkaar_Platinum.pdf pkt. 7 (sist besøkt 28.05.2018).
[86] Se BKN-1998-050 og BKN-2006-082.
[87] https://www.vipps.no/vilkar/vilkar-privat (sist besøkt 21.03.2018).

tilsier derfor at en forbruker har handlet grovt uaktsomt dersom han frivillig overlater mobiltelefonen til tredjeperson slik at det blir gjennomført uautoriserte transaksjoner.

En innvending er at det er langt vanligere å overlate mobiltelefon eller nettbrett til tredjeperson enn et betalingskort, fordi en mobil enhet har flere bruksfunksjoner enn et kort. Det virker dermed strengt at en forbruker blir ansvarlig for inntil 12.000 kroner for tap som er oppstått fordi han har lånt telefonen sin bort til en annen. Det er tale om helt ordinære handlinger som å ta en telefonsamtale, se på bilder eller bruke internett. Det vil innebære innskrenkninger i forbrukernes handlefrihet dersom det skal anses som grovt uaktsomt å la andre få tilgang til mobilen for å gjøre disse handlingene. Dette må tas til inntekt for at det ikke bør anses som grovt uaktsomt overlate mobiltelefon eller nettbrett til tredjeperson frivillig.

Dette hensynet til handlefrihet og å kunne gjøre normale, aktverdige handlinger bør etter min mening veie tyngst. Det bør altså være adgang til å gi mobiltelefon eller nettbrett til en annen person uten at man derved har handlet grovt uaktsomt hvis Vipps blir misbrukt. Enkelte krav er det likevel naturlig å stille. På samme måte som i betalingskorttilfellene må det forventes at en mobiltelefoneier holder PIN-koden til sin Vipps-profil skjult slik at den som låner enheten ikke kan logge seg inn. PIN-koden bør heller ikke oppbevares i ukamuflert form sammen med enheten når den lånes bort. I disse tilfellene er det nærliggende å anvende samme forståelse for Vipps som for betalingskort, ettersom det er handlinger som gir direkte tilgang til bruk av betalingsinstrumentet, på samme måte som for betalingskort.

En særlig utfordring med Vipps er at applikasjonen fortsetter å kjøre i bakgrunnen etter at applikasjonen er lukket, med mindre man manuelt stopper den. Dette innebærer at applikasjonen kan åpnes uten bruk av PIN-kode dersom applikasjonen nylig ble åpnet, slik at det er mulig å gjennomføre uautoriserte transaksjoner. Spørsmålet er om det er grovt uaktsomt av eieren ikke å stoppe applikasjonen før han låner enheten bort til andre. Denne situasjonen kan best sammenlignes med de tilfellene der kortholder overlater betalingskortet til en annen person som kan bruke kortet uten PIN-kode, for eksempel med signatur eller kontaktløs

verifisering. Som nevnt tidligere i dette kapitlet vil kortholder raskt komme i ansvar i disse situasjonene. Det er utvilsomt klanderverdig ikke å logge ut av Vipps før man låner. Likevel er det viktig å huske at steget fra simpel til grov uaktsomhet er større enn fra normal aktsom opptreden til simpel uaktsomhet, som vist i kapittel 3.1. Når mobiltelefon eller nettbrett i tillegg har mange flere bruksfunksjoner enn et betalingskort, bør det ikke bli sett på som grovt uaktsomt dersom eieren ikke logger ut av Vipps manuelt før han overlater enheten til noen andre.

Et annet aspekt ved uaktsomhetsvurderingen er forbrukerens personlige forutsetninger. I RG-2002-1273 uttalte lagmannsretten at det ved avgjørelsen av om forbrukeren har handlet grovt uaktsomt må legges vekt på «vedkommendes personlige evner, egenskaper og forutsetninger». Personer som har liten erfaring med mobile enheter eller har liten innsikt i teknologi vil dermed bli bedømt mildere enn personer med mye erfaring. En gruppe som skiller seg ut som mindre erfarne er eldre mennesker.[88] Samtidig er det stadig flere eldre som har nettbrett eller smarttelefon, men få som har tilgang til Vipps.[89] Vipps er dermed mindre kjent enn betalingskort blant eldre. Dette vil kunne få utslag i uaktsomhetsvurderingen, for eksempel ved at handlinger som blir ansett som grovt uaktsomme i tilknytning til betalingskort, ikke når opp til den samme terskelen i tilknytning til Vipps. På en annen side må det forventes at en person som går til anskaffelse av et betalingsinstrument setter seg inn i hvordan instrumentet fungerer, slik at terskelen ikke bør senkes mye. Et eksempel der det kan tenkes at eieren av enheten ikke har vært grovt uaktsom er dersom PIN-koden er dårlig kamuflert og blir oppbevart permanent i samme rom som mobiltelefonen. Dette vil som regel være grovt uaktsomt for betalingskort, som vist i kapittel 4.1, mens de personlige forutsetningene i et tilfelle med Vipps er dårligere.[90]

[88] https://forskning.no/2015/01/derfor-vil-han-ikke-ha-smarttelefon (sist besøkt 13.03.2018).
[89] https://forskning.no/helsepolitikk-samfunn-samfunnskunnskap-velferdsstat-teknologi-data/2016/02/de-aller-eldste-er-mye-pa (sist besøkt 13.03.2018) og https://dnbfeed.no/privatokonomi/bestemor-og-bestefar-a-laste-ned-vipps/ (sist besøkt 13.03.2018).
[90] Se også Torvund (2003) s. 1.

4.6.3 Lekkasje av PIN-koden

Ettersom mobiltelefoner og nettbrett blir mer brukt i sosiale sammenhenger enn andre betalingsinstrumenter, er det en høyere risiko for at PIN-koden kommer på avveie. Dette kan for eksempel skje ved at noen ser på skjermen mens PIN-koden blir tastet inn, eller ved at eieren av enheten røper PIN-koden til en betrodd som skal hjelpe eieren med å bruke Vipps. Eksempelet kan minne om den tidligere nevnte BKN-2003-060, der forbrukeren oppga koden til mobiltelefonen til sitt eget barnebarn, og denne koden samsvarte med PIN-koden til betalingskortet. Der hadde forbrukeren ikke opptrådt grovt uaktsomt, blant annet fordi det var upåregnelig at barnebarnet skulle finne sammenhengen.

I dette tilfellet, med mobile betalingsinstrumenter, er det imidlertid helt påregnelig at en person som vet PIN-koden kan forsøke å logge seg inn på Vipps ved en senere anledning. Dermed kommer ikke dette formildende momentet til anvendelse i denne situasjonen, hvilket tilsier at en mobileier som røper PIN-koden har handlet grovt uaktsomt. I motsetning til de situasjonene der kunden overlater mobiltelefon eller nettbrett til tredjeperson i kapittel 4.6.2, vil det heller ikke hjelpe forbrukeren at mobiltelefoner og nettbrett har et utvidet anvendelsesområde. Årsaken til dette er at dersom man er i ferd med å logge inn på Vipps og andre ser koden, eller man røper PIN-koden, har man å gjøre med et betalingsinstrument og ikke mobiltelefon eller nettbrett som sådan. På dette punktet bør derfor atferd som anses grovt uaktsomt ved misbruk av de tradisjonelle betalingsinstrumentene også anses grovt uaktsomt for misbruk av mobile betalingsinstrumenter.

4.6.4 Oppbevaring av betalingskort og mobiltelefon sammen

Som nevnt i kapittel 4.6.1 er det tilstrekkelig å ha kortnummeret som er registrert i Vipps for å lage ny PIN-kode dersom man har glemt den eksisterende koden. I tillegg er det mulig å kjøpe mobildeksel eller -etui med kortlommer, slik at mobiltelefonen og kortet oppbevares sammen. Dersom forbrukeren mister begge disse, er risikoen for misbruk følgelig svært høy, ettersom det er enkelt å skifte PIN-kode på Vipps-applikasjonen. Det må derfor vurderes om det er grovt uaktsomt å oppbevare betalingskortet som er registrert på Vipps-applikasjonen og mobiltelefon sammen. Denne vurderingen må ses i lys av finansavtaleloven § 34 første ledd

sitt krav om å ta alle «rimelige» forholdsregler for å beskytte sikkerhetsanordninger knyttet til betalingsinstrumentet. Med andre ord skal det også vurderes om risikoen for misbruk enkelt kunne elimineres av forbrukeren. Det er mange alternative måter å oppbevare et betalingskort på enn i et mobildeksel. Det finnes egne kortholdere hvor man kan oppbevare betalingskort, i tillegg til de tradisjonelle lommebøkene. Selv om deksel med kortlomme er praktisk, fremstår ikke alternativene som mindre praktiske. Dette tilsier at det er rimelig å kreve at en forbruker ikke oppbevarer betalingskortet sammen med den mobile enheten i et slikt deksel.

Finansklagenemnda har videre lagt klart til grunn at oppbevaring av PIN-kode sammen med betalingskort er grovt uaktsomt.[91] Oppbevaring av betalingskort sammen med mobiltelefon har store likhetstrekk med disse situasjonene. Selv om det kreves noen flere håndvendinger for å gjennomføre transaksjoner på Vipps sammenlignet med et betalingskort, er det forholdsvis enkelt å misbruke betalingsinstrumentet i begge situasjonene. Forskjellen til betalingskort er at mobiltelefoner og nettbrett kan ha skjermlås, men disse er ofte enkle å gjennomskue, eller blir ikke benyttet i det hele tatt.[92] Dermed er ikke risikoen for misbruk noe særlig mindre i det foreliggende tilfellet enn der kode og kort blir oppbevart sammen. Finansklagenemndas praksis på dette punkt taler klart for at også bruk av slikt deksel er grovt uaktsomt.[93]

Etter dette er det klart at det må anses som grovt uaktsom av forbrukeren å oppbevare betalingskort som er registrert på mobiltelefonens Vipps-applikasjon i deksel med kortlomme. Noe annet vil det være om forbrukeren har både betalingskortet og mobiltelefonen med seg når han går ut av huset o.l. Det er lite praktisk å måtte velge mellom å legge igjen kortet eller mobiltelefon hjemme, slik at dette ikke kan anses å være en «rimelig» forholdsregel etter § 34. Man bør imidlertid unngå å oppbevare dem i samme lomme slik at begge enkelt kan stjeles samtidig.

[91] Se kapittel 4.2.
[92] Se https://norsis.no/1-av-3-har-for-darlig-sikkerhet-pa-sin-android-enhet/ (sist besøkt 15.03.2018).
[93] Se for eksempel BKN-2014-131.

5 Avslutning

Oppgavens fokus har vært rettet mot grensen mellom simpel og grov uaktsomhet knyttet til misbruk av elektroniske betalingsinstrumenter ved enkelte typetilfeller. I kapitlene 3 og 4 ble det fastslått at spranget mellom simpel uaktsomhet og grov uaktsomhet er svært stort. Analysen av retts- og nemndspraksis viser at norske instanser stort sett opptrer lojalt til denne svært høye terskelen. I kapittel 1 reiste oppgaven bekymringer knyttet til om Norge, Sverige og Danmark har en lik forståelse av forsømmelsesvilkåret i PSD. Disse bekymringene har vist seg å være berettiget etter den komparative analysen av hvordan vilkåret forstås i de skandinaviske landene. Selv om norsk og svensk rett har en stort sett lik forståelse av vilkåret, skiller dansk rett seg ut som særdeles forbrukervennlig. Etter min mening uthuler Pengeinstitutankenævnet kravene PSD 1 og 2 stiller til kundens opptreden ved å plassere ansvaret hos finansinstitusjonen på tross av graverende atferd fra kunden. Den danske nemnda har dermed lagt til grunn en annen forståelse av direktivets bestemmelser om uautoriserte transaksjoner enn Norge og Sverige.

I siste del av kapittel 4 er det gjort rede for anvendelsen av finansavtaleloven ved misbruk av mobile betalingsinstrumenter, der Vipps er det praktisk viktigste. Som vist i kapittel 2 gjelder finansavtaleloven fullt ut ved misbruk av Vipps, med visse unntak der det er brukt biometriske data for å gjennomføre transaksjonen eller skaffe adgang til betalingsinstrumentet. I tillegg har oppgaven tatt for seg de typetilfellene jeg mener vil være de mest aktuelle når det kommer til uautoriserte transaksjoner ved bruk av Vipps, der målet har vært å trekke en grense for grov uaktsomhet. Etter min vurdering blir drøftelsen av om kunden har opptrådt grovt uaktsomt mer kompleks der betalingsinstrumentet er integrert i en mobiltelefon eller et nettbrett. Flerbruksfunksjonen til en mobiltelefon eller et nettbrett gjør at handlinger som umiddelbart ville fremstått som grovt uaktsomme når det gjelder betalingskort, bør vurderes annerledes når det er tale om Vipps. Samtidig er det ingen grunn til å legge til grunn noen annen forståelse av uaktsomhetsvilkåret dersom mobiltelefonen faktisk blir brukt som et betalingsinstrument, og ikke bare som mobiltelefon, på det tidspunktet kunden forsømmer seg. Dette kan skape bevismessige utfordringer i fremtiden, ettersom det er vanskelig å bevise om telefonen bare ble brukt som mobiltelefon, eller om den ble brukt som betalingsinstrument. Verken domstolene eller Finansklagenemnda har

imidlertid tatt stilling til denne problemstillingen i skrivende stund, men Vipps eller lignende tjenester vil spille en sentral rolle i betalingsformidlingen i fremtiden. Vi behøver dermed forhåpentligvis ikke å vente lenge før disse spørsmålene blir avklart.

Litteraturliste

Bøker

Geva, Benjamin. Payment Transactions under the EU Payment Services Directive: A U.S. Comparative Perspective i *14th Biennial Meeting of the International Academy of Commercial and Consumer Law – Bamberg, Germany – July 30 – August 3, 2008* (2009) s. 713-756.

Giertsen, Johan. *Avtaler,* Bergen: Universitetsforl., 2014.

Grøttjord, Børge og Rosén, Karl, *Finansavtaleloven med kommentarer,* Oslo: Gyldendal Norsk Forlag AS, 2014.

Krüger, Kai. «Rettsutvikling ved nemndspraksis» i *Klagenemnder – rettssikkerhet og effektivitet,* Nina Mår og Barbro Andenæs (red.), Bergen: Fagbokforlaget, 2008, s. 103-122.

Sejersted, Fredrik, Finn Arnesen, Sten Foyn mfl. *EØS-rett*, 3. utg., Oslo: Universitetsforl., 2011.

Sundberg, Jacob W. F. «Om generalklausuler» i *Festskrift til Jan Hellner,* Ulf Bernitz, Bill W. Dufva, Kurt Grönfors mfl. (red.), Stockholm: P A Norstedt & Söners Förlag, 1984, s. 659-680.

Von Eyben, Bo. *Begrebet grov uaktsomhed på forskellige retsområder,* Det 33. nordiske juristmøte i København 1993 (1993) s. 587-650.

Artikler og avhandlinger

Torvund, Olav. *Kamuflering av PIN-koder: Noen refleksjoner om Borgarting lagmannsretts dom i RG-2002-1273 og senere praksis fra Bankklagenemnda,* Lov&Data (2003) s. 1-2.

Bergström, Andreas. *Betalningsansvar vid obehöriga transaktioner,* Stockholm, 2010.

Domsregister

Høyesterettspraksis

Rt. 2004 s. 499

Rt. 2004 s. 1942

Rt. 2008-1360

HR-2016-1464-A

Underrettspraksis

RG-2002-1273

EU-domstolen

Case C-616/11 T-Mobile Austria GmbH v Verein für Konsumenteninformation
ECLI:EU:C:2014:242

Lover og EU-kilder

Norske lover

Finansavtaleloven	Lov av 26. juni 1999 om finansavtaler og finansoppdrag
Avtaleloven	Lov av 31. mai 1918 om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer

Utenlandske lover

Betalingsloven	Lov nr. 652 af 8. juni 2017 om betalinger

Lagen om obehöriga transaktioner	Lag (2010:738) om obehöriga transaktioner med betalningsinstrument

Traktater

TEU	Traktaten om den Europeiske Union. Konsolidert versjon 2016 (EUT/2016/C 202/01)
TEUV	Traktaten om den Europeiske Unions virkemåte. Konsolidert versjon 2016 (EUT 2016/C 202/01)

EU-direktiver

Betalingstjenestedirektiv 1	Europaparlaments- og rådsdirektiv 2007/64/EF av 13. november 2007 om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF samt oppheving av direktiv 97/5/EF [Betalingstjenestedirektivet]
Betalingstjenestedirektiv 2	Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om opphevelse av direktiv 2007/64/EF

Andre EU-kilder

Recommendation 88/590/EEC	Kommissionens henstilling af 17. november 1988 om betalingssystemer, herunder navnlig om forholdet mellem kortindehaver og kortutsteder

Lovforarbeider

Norske lovforarbeider

Snr. 17/4746	Høringsnotat – revisjon av finansavtaleloven
Ot.prp.nr.94 (2008-2009)	Om lov om endringer i finansavtaleloven mv. (gjennomføring av de privatrettslige bestemmelsene i direktiv 2007/64/EF)
Ot.prp.nr.41 (1998-1999)	
NOU 1994:19	Finansavtaler og finansoppdrag

Utenlandske lovforarbeider

Prop. 2009/10:122	Obehöriga transaktioner med betalningsinstrument
Prop. 1976/77:123	Förslag till konsumentkreditlag m.m.

Nemndspraksis

Finansklagenemnda

BKN-2017-035

BKN-2017-001

BKN-2016-496

BKN-2016-452

BKN-2016-093

BKN-2015-321

BKN-2015-019

BKN-2014-131

BKN-2012-541

BKN-2010-062

BKN-2006-084

BKN-2006-082

BKN-2006-080

BKN-2006-015

BKN-2004-116

BKN-2004-077

BKN-2003-060

BKN-2003-049

BKN-2001-052

BKN-2001-017

BKN-2000-050

BKN-1998-050

BKN-1997-031

BKN-1994-061

Allmänna Reklamationsnemnden

2002-8212

2001-4153

1999-2533

1999-1705

Pengeinstitutankenævnet

320/2007

78/2006

205/2005

14/2002

333/2000

386/1997

685/1992

420/1991

Markedsrådet

MR-2015-1018

Internett

Aftenposten. *Alle bankene er snart med i Vipps*, https://www.aftenposten.no/okonomi/i/Pk2k0/Alle-bankene-er-snart-med-i-Vipps

Danske Bank. *Avtalevilkår for kontoavtale – forbrukerforhold*, https://danskebank.no/nb-no/Privat/Documents/Generelle-vilkaar_Platinum.pdf

DnB. *Vilkår for Visa og Mastercard*, https://www.dnb.no/portalfront/dnb/nedlast/privat/avtaler/kontoavtale-vilkaar-visa-mastercard-E.pdf?popup=true

DnB Nyheter. *Nå skal Bestemor og Bestefar på Vipps*, https://dnbfeed.no/privatokonomi/bestemor-og-bestefar-a-laste-ned-vipps/

DnB Nyheter. *Unngå å bli lurt eller svindlet,* https://dnbfeed.no/privatokonomi/unnga-a-bli-lurt-eller-svindlet/

E24. *Rekordår for kortsvindel i 2016: Over 17 milliarder tapt i Europa,* https://e24.no/lov-og-rett/bank/rekordaar-for-kortsvindel-i-2016-over-17-milliarder-tapt-i-europa/24095074

European Commission. *Your questions on PSD,* http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq-2008_11_20_en.pdf

Finansklagenemnda. *Søk etter uttalelser*, https://publisering.finkn.no/keywords/4/AZ01

Forskning.no. *Derfor vil ikke bestefar ha smarttelefon,* https://forskning.no/2015/01/derfor-vil-han-ikke-ha-smarttelefon

Forskning.no. *De eldste er mye på internett,* https://forskning.no/helsepolitikk-samfunn-samfunnskunnskap-velferdsstat-teknologi-data/2016/02/de-aller-eldste-er-mye-pa

Harstad Tidende. *Ble svindlet for 5.000 kroner på Vipps – uten å ha appen,* https://www.ht.no/nyheter/2016/02/18/Ble-svindlet-for-5.000-kroner-p%C3%A5-Vipps-uten-%C3%A5-ha-appen-12173934.ece

Nordea. *Del E (n) av kontoavtalen,* https://www.nordea.no/Images/57-82383/Cards%20-%20Avtalevilk%C3%A5r%20Nordea%20Bankkort.pdf

Norsk senter for informasjonssikring. *1 av 3 har for dårlig Android-sikkerhet,* https://norsis.no/1-av-3-har-for-darlig-sikkerhet-pa-sin-android-enhet/

NRK. *Falsk TV-montør svindlet eldre par,* https://www.nrk.no/buskerud/_kan-jeg-fa-pin-koden-din__-1.11834850

Sparebanken Vest. *Avtalevilkår for betalingskort (debetkort) forbruker,* https://www.spv.no/-/media/Files/kort/avtalevilkar/Avtale-om-betalingskort.pdf

Vipps. *Vilkår Privat,* https://www.vipps.no/vilkar/vilkar-privat

Vipps. *Generelle spørsmål om Vipps – Spørsmål og svar på det aller meste vedrørende Vipps for deg som privatperson,* https://www.vipps.no/sporsmal