NOU Norges offentlige utredninger 2008: 21

Nettbankbasert betalingsoverføring

Utredning nr. 21 fra Banklovkommisjonen

Norges offentlige utredninger 2008

Seriens redaksjon:
Departementenes servicesenter
Informasjonsforvaltning

---

1. Kvinner og homofile i trossamfunn.
   Barne- og likestillingsdepartementet.

2. Fordeling av inntekter mellom regionale helseforetak.
   Helse- og omsorgsdepartementet.

3. Sett under ett.
   Kunnskapsdepartementet.

4. Fra ord til handling.
   Justis- og politidepartementet.

5. Retten til fiske i havet utenfor Finnmark.
   Fiskeri- og kystdepartementet.

6. Kjønn og lønn.
   Barne- og likestillingsdepartementet.

7. Kulturmomsutvalget.
   Finansdepartementet.

8. Bourbon Dolphins forlis den 12. april 2007.
   Justis- og politidepartementet.

9. Med barnet i fokus.
   Barne- og likestillingsdepartementet.

10. Om grunnlaget for inntektsoppgjørene 2008.
    Arbeids- og inkluderingsdepartementet.

11. Yrkessykdommer.
    Arbeids- og inkluderingsdepartementet.

12. Revisjonsplikten for små foretak.
    Finansdepartementet.

13. Eierkontroll i finansinstitusjoner.
    Finansdepartementet.

14. Samstemt for utvikling?
    Utenriksdepartementet.

15. Barn og straff.
    Justis- og politidepartementet.

16. Om foretaksstyring og tiltak mot manipulering av finansiell informasjon.
    Finansdepartementet.

17. Skift og turnus – gradvis kompensasjon for ubekvem arbeidstid.
    Arbeids- og inkluderingsdepartementet.

18. Fagopplæring for framtida.
    Kunnskapsdepartementet.

19. Fiskefartøyet "Western"s forlis 6. februar 1981.
    Justis- og politidepartementet.

20. Skadeforsikringsselskapenes virksomhet.
    Finansdepartementet.

21. Nettbankbasert betalingsoverføring.
    Justis- og politidepartementet.

NOU Norges offentlige utredninger **2008: 21**

Nettbankbasert betalingsoverføring

Utredning nr. 21 fra Banklovkommisjonen

Utredning fra Banklovkommisjonen oppnevnt ved kongelig resolusjon 6. april 1990.
Avgitt til Justis- og politidepartementet 15. desember 2008.

Departementenes servicesenter
Informasjonsforvaltning

Oslo 2008

ISSN 0333-2306
ISBN 978-82-583-0995-3

Lobo Media AS

Til Justis- og politidepartementet

I brev av 13. mars 2007 ga Finansdepartementet i samråd med Justisdepartementet Banklovkommisjonen i oppdrag å vurdere spørsmålet om sikkerhet ved bruk av nettbank og behovet for endringer i finansavtaleloven, herunder ansvarsbegrensning for bankkunder. Banklovkommisjonen legger med dette frem sin Utredning nr. 21, NOU 2008: 21 Nettbankbasert betalingsoverføring, med utkast til endringer i lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven).

Banklovkommisjonen mener at behovet for ansvarsregulering når det gjelder tap som har oppstått ved bruk av nettbasert betalingstjeneste, gjør seg gjeldende i tilfelle både av feilbruk fra kundens side og av uvedkommendes misbruk av nettbankkonti. Bruk av nettbasert betalingsoverføring medfører ulike, men typiske risiki som fra tid til annen vil føre til tap for kunder. Det er lagt opp til en ansvarsregulering som samlet sett vil gi en rimelig og balansert tapsfordeling mellom kunde og nettbank, og som også skal oppfordre kunder til å utvise aktsomhet og forsiktighet ved bruk av nettbasert betalingstjeneste.

Banklovkommisjonen foreslår i utredningen at det tas inn et nytt avsnitt Va i kapittel 2 i finansavtaleloven som fastlegger ansvarsfordelingen i tilfelle av utilsiktet og urettmessig bruk av nettbasert betalingstjeneste. Utkast til nye lovbestemmelser bygger i stor grad på de prinsipper som ligger til grunn for bestemmelsene i finansavtaleloven §§ 34 flg., særlig reglene om betalingskort i finansavtaleloven § 35. Lovutkastet innebærer at kunden som hovedregel bare skal bære en del av tapet ved utilsiktede eller urettmessige betalingsoverføringer som følge av feilbruk eller misbruk av nettbaserte betalingstjenester (egenandelsmodellen). I tilfeller hvor kunden har utvist grov uaktsomhet når det gjelder bruk av nettbasert betalingstjeneste eller oppbevaring av nødvendig brukerlegitimasjon, skal imidlertid kunden ha et vesentlig høyere ansvar, og lovutkastet inneholder også enkelte bestemmelser som i særlige tilfelle medfører at kunden selv må bære hele tapet.

Banklovkommisjonens forslag er enstemmig.

Oslo 18. november 2008

Erling Selvig
Leder

Olav Breck	Ottar Dalsøren	Sverre Dyrhaug
Kjersti Elvestad	Eystein Gjelsvik	Arnhild Dordi Gjønnes
Øivind Fegth Knutsen	Øystein Løining	Anne-Lise Løfsgaard
Per Melsom	Anne Nesheim Egeberg	Solveig Nordkvist
Astrid Nyberget	Erling G. Rikheim	Marius Ryel
Rolf A. Skomsvold	Kristin Skrede	Per Anders Stalheim
Liv Synnøve Taraldsrud	Bente Øverli	

Jørgen Keiserud
(fungerende hovedsekretær)

Kari Lærum

Lise Ljungmann Haugen
(hovedsekretær, permisjon)

Innhold

Kapittel 0
Sammendrag

0.1 Sammendrag

0.1.1 Innledning

Banklovkommisjonens Utredning nr. 21, NOU 2008: 21 Nettbankbasert betalingsoverføring, inneholder forslag til endringer i lov om finansavtaler og finansoppdrag av 25. juni 1999 nr. 46 (finansavtaleloven).

I mandat av 13. mars 2007 ga Finansdepartementet i samråd med Justisdepartementet Banklovkommisjonen i oppdrag å vurdere spørsmålet om sikkerhet ved bruk av nettbank og behovet for endringer i finansavtaleloven, herunder ansvarsbegrensning for bankkunder. Mandatet er inntatt i avsnitt 1.1 nedenfor. Som følge av prosessen med implementeringen av direktiv 2007/64/EF (betalingstjenestedirektivet), oppstod det et behov for presisering av mandatet. Spørsmål i forhold til dette og nærmere avklaringer, er det redegjort for i avsnitt 1.2.

For å få et best mulig grunnlag for behandling og vurdering av hvordan et regelverk for bruk av nettbasert betalingstjeneste bør utformes, herunder særlig virkemåten for og risikoen ved bruk av nettbank, har *Banklovkommisjonen* trukket en arbeidsgruppe bestående av representanter fra noen store bankinstitusjoner, Finansnæringens Hovedorganisasjon, Sparebankforeningen, Forbrukerombudet og Forbrukerrådet inn i det forberedende arbeidet.

0.1.2 Bakgrunnen for arbeidet

I 1994 foreslo *Banklovkommisjonen,* i sin Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag), regler om finansavtaler og finansoppdrag. Lovforslaget ble i stor grad lagt til grunn i det videre lovforarbeidet og ble vedtatt som lov 25. juni 1999 nr. 25 (finansavtaleloven). På dette tidspunkt var det kun et begrenset innslag av nettbaserte betalingsoverføringsformer. Det var særlig betalingsoverføring ved bruk av betalingskort, det vil si debet- og kredittkort, som utpekte seg, og som *Banklovkommisjonen* fant grunn til å regulere etter nærmere bestemte regler, jf. finansavtaleloven §§ 35 flg. *Banklovkommisjonen* var imidlertid – på dette tidspunktet – klar over utviklingen av en ny form for betalingsoverføring som gjorde det mulig å gi betalingsinstrukser til sin bank via en hjemmeterminal, såkalt «hjemmebank», jf. blant annet Banklovkommisjonens Utredning nr. 1 side 71. Denne form for betalingsoverføring er det vi nå kjenner som nettbank, og som brukes i utstrakt grad ved siden av telefonbank. Behovet for en regulering av disse betalingsoverføringsmekanismene var forutsett, og *Banklovkommisjonen* foreslo i den forbindelse en forskriftshjemmel i finansavtaleloven § 35 sjette ledd om at de særskilte reglene for betalingskort helt eller delvis kunne gjøres gjeldende for andre typer betalingsinstrumenter.

En utredning av behovet for om en nærmere regulering av slike betalingsoverføringsformer skulle innføres, ble utsatt blant annet i påvente av EU-direktivet om betalingstjenester. Som følge av en konkret sak i 2007 hvor en kunde utilsiktet, det vil si ved feilbruk av betalingstjenesten, hadde overført et større beløp til gal mottaker, ble spørsmålet om sikkerheten ved bruk av nettbank reist på nytt. Underveis i utredningsarbeidet ble det imidlertid også lagt opp til at spørsmål om urettmessige nettbaserte betalingsoverføringer kunne utredes nærmere, det vil si misbruk av nettbaserte betalingstjenester. Det vises her til avsnitt 1.2. Om regelverkets plassering i norsk rett vises det til avsnitt 6.1.3.

0.1.3 Banklovkommisjonens vurderinger og forslag

Banklovkommisjonen mener at behovet for ansvarsregulering når det gjelder tap som har oppstått ved bruk av nettbasert betalingstjeneste, gjør seg gjeldende både ved feilbruk fra kundens side og uvedkommendes misbruk av nettbankkonti. Bruk av nettbasert betalingsoverføring medfører ulike, men typiske risiki som fra tid til annen vil føre til tap for kunder. *Banklovkommisjonen* har ansett slike regler som et viktig innslag i dagens lovgivning, særlig i lys av det store antall av den norske befolkning som benytter seg av nettbaserte

betalingstjenester, som for eksempel nettbank og telefonbank. I takt med den økte bruken av Internett, antar *Banklovkommisjonen* videre at de nettbaserte betalingstjenestene vil være den praktisk sett dominerende betalingstjeneste for regningsbetaling i årene fremover. Brukerkretsen vil således utvides, og brukerkollektivet vil omfatte personer med varierende teknisk og datamessig innsikt ut fra de enkeltes personlige forutsetninger. Selv om antall betalingsoverføringer ved bruk av slike tjenester i dag er på et høyt nivå, må det derfor forventes en betraktelig økning av slike betalingsoverføringer i tiden fremover. Det vises til avsnitt 6.1.3. En nærmere beskrivelse av virkemåten for nettbank og telefonbank er gitt i avsnittene 5.2.1 og 5.2.2.

Banklovkommisjonen foreslår i utredningen at det tas inn et nytt avsnitt Va i kapittel 2 i finansavtaleloven som fastlegger ansvarsfordelingen i tilfelle av utilsiktet og urettmessig bruk av nettbasert betalingstjeneste. Utkast til nye lovbestemmelser bygger i stor grad på de prinsipper som ligger til grunn for bestemmelsene i finansavtaleloven §§ 34 flg., særlig reglene om betalingskort i finansavtaleloven § 35. Dette har sin bakgrunn i at nettbasert betalingsoverføring også kan iverksettes ved hjelp av en form for brukerlegitimasjon som innebærer en forhøyet risiko for at det oppstår tap. Lovutkastet innebærer at kunden som hovedregel bare skal bære en del av tapet ved utilsiktede eller urettmessige betalingsoverføringer som følge av feilbruk eller misbruk av nettbaserte betalingstjenester (egenandelsmodellen).

Etter lovutkastet skal kunden ha en objektiv, men begrenset egenrisiko (ansvar) for utilsiktede og urettmessige nettbaserte betalingsoverføringer som har oppstått som følge av feilbruk eller misbruk. *Banklovkommisjonen* mener at en slik regel vil oppfordre kunder til å utvise nødvendig forsiktighet og opptre med rimelig aktsomhet i sin bruk av nettbaserte betalingsoverføringstjenester. Den objektive egenandelen gjelder imidlertid ikke dersom årsaken må tilskrives sikkerhetsmangler ved nettbanksystemet eller andre forhold som kunden ikke kan lastes for. Det kan ikke utelukkes at institusjonenes systemer ikke tilfredsstiller de krav som med rimelighet må stilles til kontroll og sikkerhet for å motvirke at utilsiktede eller urettmessige betalingsoverføringer iverksettes. Med utgangspunkt i produktansvarsreglene, har *Banklovkommisjonen* derfor fremmet forslag om at den objektive egenandelen ikke gjelder dersom tapet har oppstått som følge av at institusjonens betalingstjenester ikke byr den sikkerhet som en bruker eller allmennheten med rimelighet kunne vente.

Banklovkommisjonen har videre foreslått at kunden også skal være ansvarsfri dersom tilegnelsen av nødvendig brukerlegitimasjon har forekommet på en måte som tilsier at kunden ikke bør pålegges ansvar. Det vises til lovutkastet § 37b første ledd annet punktum in fine i kapittel 9, og merknader til bestemmelsen i kapittel 8.

I tilfeller hvor kunden har utvist grov uaktsomhet når det gjelder bruk av nettbasert betalingstjeneste eller oppbevaring av nødvendig brukerlegitimasjon, og dette har ført til tap som følge av at utilsiktede eller urettmessige betalingsoverføringer er iverksatt, skal imidlertid kunden ha et vesentlig høyere ansvar. Egenandelen er her satt noe høyere enn for betalingskortene. Formålet har vært å legge til rette for en rimeligere tapsfordeling i visse særlige tilfelle, og statuere at nettbaserte betalingstjenester har så mange iboende risiki at kunden må opptre aktsomt og forsiktig i sin bruk av tjenesten. *Banklovkommisjonen* understreker at det ved vurderingen av hvilket ansvar kunden selv bør ha fordi kundens handlemåte innebærer en grov tilsidesettelse av kundens egen plikt til å unngå at tap oppstår, vil kunne få betydning for hvilken feil kunden måtte ha utvist i det enkelte tilfelle. Lovutkastet inneholder også enkelte bestemmelser som i særlige tilfelle medfører at kunden selv må bære hele tapet. Det vises her til avsnittene 6.3.2 og 6.3.3.

Banklovkommisjonen har som nevnt lagt vekt på prinsippene i finansavtaleloven §§ 34 flg. Bestemmelsene om lemping av kontohaverens ansvar samt bestemmelsen om reklamasjon og tilbakeføring, er i hovedsak også videreført. Når det gjelder krav til dokumentasjon, har *Banklovkommisjonen,* både av prosessøkonomiske og samfunnsøkonomiske hensyn, sett det som hensiktsmessig at kundens krav om tilbakeføring er begrunnet og at kunden i tillegg plikter å gi opplysninger til institusjonen om, og på hvilken måte, det er gjort forsøk på å få betalingsmottakeren til å tilbakeføre beløp som utilsiktet eller urettmessig er overført til mottakeren. Det vises her til avsnitt 6.3.6 og lovutkastet § 37d annet ledd.

0.2 English Summary

0.2.1 Introduction

The Banking Law Commission's Report no. 21, NOU 2008: 21 Payment transfers in online banking services, contains proposals for amendments to the Act on Financial Agreements and Financial

Assignments of 25 June 1999 no. 46 (the Financial Agreements Act).

In the terms of reference of 13 March 2007 the Norwegian Ministry of Finance, in consultation with the Ministry of Justice, mandated the Banking Law Commission to consider the question of security in use of online banking services and the need for amendments to the Financial Agreements Act, including limitation of liability for bank customers. The terms of reference are incorporated in Section 1.1 below. In consequence of the process of implementation of Directive 2007/64/EC (the payment services directive), there arose a need to clarify the terms of reference. Questions related to this and further clarifications are described in Section 1.2 below.

In order to obtain the best possible basis on which to consider and evaluate how regulations for use of online payments service should be designed, including in particular the functioning of and risk involved in the use of online banking services, *the Banking Law Commission* has drawn upon a working party consisting of representatives of some big bank institutions, the Norwegian Financial Services Association (FNH), the Norwegian Savings Banks Association, the Consumer Ombudsman and the Consumer Council, into the preparatory work.

0.2.2 Background for the report

In 1994 *the Banking Law Commission,* in its Report no. 1 (NOU 1994: 19 Financial Agreements and Financial Assignments), proposed rules on financial agreements and financial assignments. The main lines of the recommendation were continued in the drafting work and were passed as Act No. 25 of 25 June 1999 (the Financial Agreements Act). At that time the extent of online payments transfers was limited. What stood out particularly was payments transfer via use of payment cards, that is to say direct-debit and credit cards, and it was this that *the Banking Law Commission* found reason to regulate under special rules, confer Sections 35 ff. of the Financial Agreements Act. *The Banking Law Commission* was however – at that time – aware of the development of a new form of payments transfer that made it possible to issue payment instructions to one's bank via a home terminal, the so-called «home banking», confer inter alia the Banking Law Commission's Report no. 1 page 71. This form of payments transfer is what we now know as «online banking services», and is used extensively in parallel to telephone banking. The need to regulate these payment transfer mechanisms was foreseen and in this connection *the Banking Law Commission* proposed an authorisation for regulations in Section 35 sixth paragraph of the Financial Agreements Act to the effect that the special rules for payment cards could, wholly or in part, be made applicable to other kinds of payment instruments.

A report on whether more detailed regulation of such forms of payments transfer was needed was deferred inter alia in expectation of the EU directive on payment services. In consequence of a specific case in 2007 in which a customer had unintentionally – that is, by erroneous use of the payment service – transferred a large sum of money to the wrong recipient, the question of security in use of online banking services was raised anew. Along the way in the report work, however, it was suggested that the question of unlawful online payments transfers could be studied more closely, that is, the abuse of online payment services, see Section 1.2 below. For the incorporation of the regulations in Norwegian law see Section 6.1.3 below.

0.2.3 The Banking Law Commission's assessments and recommendations

The Banking Law Commission considers that the need for regulation of liability for losses caused by the use of online payment services applies to both error on the part of the customer and unauthorised persons' abuse of online banking accounts. Use of online payments transfer involves various, but typical, risks that from time to time will lead to losses for customers. *The Banking Law Commission* regards such rules as an important element of present legislation, particularly in the light of the large number of Norwegians who make use of online payment services, such as for example online banking services and telephone banking. In step with the increased use of the Internet, *the Banking Law Commission* also assumes that the online payment services will be the practically-speaking dominant method of paying bills in the years to come. The circle of users will be growing constantly, and the user collectivity will include individuals with variable technical and computer knowledge and personal skills. Even if the number of payments transfers involved in the use of such services is currently at a high level, a considerable increase of such payments transfers may therefore be expected in future, see Section 6.1.3 below. A detailed description of the mode of functioning of online banking services and telephone banking is provided in Sections 5.2.1 and 5.2.2 below.

In its report *the Banking Law Commission* recommends that a new Section Va be included in Chapter 2 of the Financial Agreements Act that lays down the division of liability in the case of unintentional and unlawful use of online payment services. The draft statutory provision is based largely on the principles underlying Sections 34 ff. of the Financial Agreements Act, particularly the rules on payment cards in Section 35 of the Financial Agreements Act. This is because online payments transfer may also be performed via a form of User ID that involves an increased risk of loss. The draft amendment means that, as a main rule, the customer shall bear only a part of the loss from unintentional or unlawful payments transfers in consequence of erroneous use or misuse of online payment services (the «deductible» model).

Under the draft amendment the customer shall have an objective, but limited, own risk (liability) for unintentional and unlawful online payments transfers caused by erroneous use or abuse. *The Banking Law Commission* considers that such a rule will challenge customers to employ the requisite prudence and to act with due care in their use of online payment transfer services. The objective deductible will not, however, apply if the cause can be assigned to security defects in the online banking services system or other factors for which the customer cannot be blamed. It cannot be ruled out that the institutions' systems do not satisfy the requirements that can reasonably be made of control and security in order to prevent the occurrence of unintentional or unlawful payments transfers. Taking the product liability rules as its point of departure, *the Banking Law Commission* has therefore recommended that the objective deductible should not apply if the loss has arisen in consequence of the failure of the institution's payment services to offer the security that a user or the public can reasonably expect. *The Banking Law Commission* also recommends that the customer also be free from liability if the requisite User ID has occurred in a manner that dictates that the customer not be liable. See the draft Section 37b first paragraph second period at the end of Chapter 9, and comments on the provision in Chapter 8.

In cases where the customer has displayed gross negligence in his use of online payment services or storage of requisite User ID, and this has led to loss in consequence of unintentional or unlawful payments transfers, however, the customer shall have substantially greater liability. Here the deductible is pitched higher than for the payment cards. The object is to facilitate a more reasonable allocation of loss in certain special cases, and to signal that online payment services contain so many inherent risks that the customer must behave prudently and with due care in his use of the service. *The Banking Law Commission* would emphasise that consideration of what liability the customer himself ought to have, on the grounds that the customer's actions amounted to a gross violation of the customer's own duty to avoid loss, should be based on what mistakes the customer made in each individual case. The draft also contains certain provisions that in special cases mean that the customer himself must bear the entire loss. See here Sections 6.3.2 and 6.3.3 below.

The Banking Law Commission has, as mentioned above, emphasised the principles of Sections 34 ff of the Financial Agreements Act. The principles for discretionary change to the account-holder's liability and the provisions for complaint and recovery have by and large also been continued. As regards documentation requirements, *the Banking Law Commission,* for reasons of both trial costs and societal interests, considers it reasonable that demands for recovery be justified and that the customer be obliged in addition to give information to the institution about whether, and if so how, he has attempted to induce the payment recipient to repay sums unintentionally or unlawfully transferred to said recipient. See here Section 6.3.6 below and Section 37d second paragraph of the draft.

0.3 Banklovkommisjonens sammensetning

Banklovkommisjonen har ved avgivelsen av denne utredning følgende 21 medlemmer:

- Professor dr. juris Erling Selvig, leder (Universitetet i Oslo)
- Avdelingsdirektør Olav Breck (Sparebankforeningen i Norge)
- Banksjef Ottar Dalsøren (Sparebanken Sogn og Fjordane/ Finansforbundet)
- Direktør Sverre Dyrhaug (Finansnæringens Hovedorganisasjon)
- Seksjonssjef Kjersti Elvestad (Kredittilsynet)
- Økonomisk rådgiver Eystein Gjelsvik (Landsorganisasjonen i Norge)
- Advokat Arnhild Dordi Gjønnes (Næringslivets Hovedorganisasjon)
- Advokat Øivind Fegth Knutsen (Advokatfirmaet Fegth Knutsen & Co DA)
- Administrerende direktør Anne-Lise Løfsgaard (Finansieringsselskapenes forening)

- Avdelingsdirektør Øystein Løining (Finansdepartementet)
- Direktør Per Melsom, Oslo
- Rådgiver Anne Nesheim Egeberg (Forbrukerrådet)
- Autorisert regnskapsfører Solveig Nordkvist (Handels- og Servicenæringens Hovedorganisasjon)
- Seniorrådgiver Astrid Nyberget (Konkurransetilsynet)
- Avdelingsdirektør Erling G. Rikheim (Finansdepartementet)
- Direktør Marius Ryel (Norges Bank)
- Generalsekretær Rolf A. Skomsvold (Norske Pensjonskassers Forening)
- Advokat Kristin Skrede (DnB NOR ASA)
- Seniorrådgiver Per Anders Stalheim (Barne- og likestillingsdepartementet)
- Sorenskriver Liv Synnøve Taraldsrud (Eiker, Modum og Sigdal tingrett)
- Seksjonssjef Bente Øverli (Forbrukerombudet)

Sekretariatet har, ved utarbeidelsen av denne utredningen, bestått av:

- Førstekonsulent Jørgen Keiserud, fungerende hovedsekretær (Finansdepartementet)
- Bankrådgiver Kari Lærum (Norges Bank)
- Seniorrådgiver Lise Ljungmann Haugen, hovedsekretær (permisjon) (Kredittilsynet)

Del I
Bakgrunnen for lovarbeidet

Kapittel 1
Oppdraget

1.1 Mandat

Finansdepartementet har i samråd med Justisdepartementet gitt Banklovkommisjonen i oppdrag å vurdere spørsmålet om sikkerhet ved bruk av nettbank og behovet for endringer i finansavtaleloven, herunder spørsmålet om en ansvarsbegrensning for bankkunder. I *brev av 13. mars 2007* skriver Finansdepartementet følgende:

> «Det har i den senere tid vært reist spørsmål om sikkerheten ved bruk av nettbank. Bankklagenemnda kom i sak 2007-015 og sak 2007-016 til at en kunde som overførte et beløp til gal mottaker, ikke kunne kreve tapet erstattet – verken av egen bank eller av mottakerens bank.
>
> Bruk av betalingstjenester generelt – giro, telefonbank eller nettbank – kan innebære at kunden selv må fylle ut nødvendig informasjon (mottakerens kontonummer og det beløpet som ønskes overført). Kunden kan i den forbindelse fylle ut galt kontonummer eller galt beløp. Dette kan lede til at beløpet overføres til en annen mottaker enn den kunden hadde tenkt å overføre beløpet til, eller til at mottakeren mottar et for stort beløp. Dersom mottakeren ikke frivillig tilbakefører beløpet, kan dette medføre tap for kunden, jf. for så vidt situasjonen i de to nevnte sakene fra Bankklagenemnda.
>
> Finansavtaleloven har i kapittel 2 avsnitt IV regler om føring av konto, herunder regler om retting av feilaktige godskrivninger og belastninger. Disse reglene retter seg mot feil på institusjonens side. Spørsmålet her gjelder feil som kunden selv begår. Banklovkommisjonen bes vurdere om det er behov for regler om at kunden ved egne feil helt eller delvis skal holdes skadesløs, det vil si om finansinstitusjonen bør bære hele eller deler av tapet i slike tilfeller.
>
> Banklovkommisjonen bes beskrive og vurdere risikoen for at kunden selv gjør feil ved betalingsoverføring. Kommisjonen bes i den forbindelse beskrive hva feilen kan bestå i og om risikoen for feil er større ved enkelte former for betalingsoverføring enn ved andre. Kommisjonen bes på denne bakgrunn vurdere behovet for regulering, herunder om det er behov for særlig regulering for enkelte typer betalingsformidling. Når det gjelder risikoen for feil ved bruk av nettbank, bes kommisjonen særlig om å vurdere dette i forhold til de tiltakene som finansnæringen selv har iverksatt, det vil si om det i tillegg til næringens egne tiltak er behov for regulering. Finansnæringen skal innen utgangen av mars 2007 ha gjennomført disse tiltakene, og Kredittilsynet skal innen 20. april 2007 komme med en vurdering av disse. Kommisjonen skal på dette punktet avvente Kredittilsynets vurdering av tiltakene.
>
> Banklovkommisjonen bes utrede hvordan en eventuell regulering av «tapsfordelingen» mellom kunden og institusjonen kan skje ved kundens egne feil. Kommisjonen skal i den forbindelse vurdere ulike mulige løsninger, herunder, men ikke begrenset til, følgende alternativer:
>
> 1. *Finansinstitusjonen kan bli erstatningsansvarlig dersom den tilbyr betalingssystemer med manglende sikkerhet eller lignende.* Kommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere hvordan en slik eventuell regulering forholder seg til alminnelige erstatningsregler, og på denne bakgrunn vurdere behovet for en lovregulering. Kommisjonen bes vurdere hvordan en eventuell regel om dette kan utformes – særlig om det er hensiktsmessig med en mer skjønnsmessig regel, eller om man bør stille mer konkrete krav til sikkerheten i systemet for betalingsoverføring. Kommisjonen bes om å gjøre rede for hvordan en slik regel vil fungere i praksis.
>
> 2. *Kunden har en begrenset tapsrisiko (en egenandel) ved egne feil, det vil si at finansinstitusjonen må dekke tap over et gitt beløp.* Kommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere hva slags dokumentasjon eller bevis som skal kreves for at institusjonen skal måtte foreta en tilbakeføring til kunden. Det skal videre vurderes om institusjonens plikt til å tilbakeføre beløpet skal inntre straks det har skjedd en feil, eller om institusjonen bare skal ha en slik plikt dersom kunden har lidd et tap. Kommisjonen bes vurdere om og i hvilken grad en slik regel innebærer fare for svindel. Kommisjonen bes vurdere hvordan en slik regel kan utformes. I

den forbindelse bes kommisjonen særskilt vurdere om regelen kan avgrenses til feil som skyldes eventuell risiko ved systemet for betalingsformidling, eller om regelen også vil måtte omfatte andre feil, for eksempel feil som skyldes at kunden har misoppfattet et kontonummer. Kommisjonen bes i den forbindelse også om å gjøre rede for mulige bevis- og avgrensningsspørsmål som kan oppstå. Kommisjonen skal videre vurdere hva som eventuelt vil være en rimelig fordeling av tapet mellom kunden og institusjonen.

3. *Finansinstitusjonen gis en rett til å korrigere feilbetalingen, jf. for så vidt finansavtaleloven § 31 om feil som skyldes institusjonens egne forhold.* Kommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere om det bør være tidsmessige begrensninger eller andre former for skranker for institusjonens korreksjonsadgang. Kommisjonen bes videre vurdere hva slags dokumentasjon eller bevis som skal kreves for at banken skal kunne foreta en korreksjon. Kommisjonen bes i den forbindelse vurdere om det er hensiktsmessig at institusjonen ved å foreta en korreksjon, bringes inn i forholdet mellom betaleren og mottakeren, jf. for eksempel en situasjon der betaleren og mottakeren er uenig om beløpets størrelse er korrekt. Kommisjonen bes videre vurdere om og eventuelt i hvilken grad institusjonen løper en risiko dersom den foretar korreksjon på feilaktig grunnlag.

Uavhengig av hvordan Kommisjonen ser på behovet for lovregulering, skal den legge frem forslag til lovbestemmelser på bakgrunn av de tre mulige løsningene nevnt ovenfor og på bakgrunn av eventuelle andre mulige løsninger.

I EU arbeides det for tiden med et direktiv om betalingstjenester, jf. KOM(2005) 603. Direktivforslaget er til behandling i Europaparlamentet og Rådet, men det er ikke klart når et endelig direktiv vil bli vedtatt. Banklovkommisjonens utredning og vurdering skal ta hensyn til direktivforslaget, med de endringer som eventuelt er eller vil bli foreslått. Kommisjonen skal særlig vurdere forholdet til direktivforslaget artikkel 66, og hvordan de mulige alternative reguleringsforslagene forholder seg til denne bestemmelsen særskilt og direktivet generelt.

Kommisjonen skal vurdere de økonomiske og administrative konsekvenser av de ulike forslagene.

Kommisjonen skal avgi sin utredning innen 31. desember 2007.»

Selv om mandatets tittel er begrenset til nettbank, er det også forutsatt at Banklovkommisjonen skal beskrive og vurdere risikoen for at kunden selv gjør feil ved betalingsoverføring generelt. I tillegg til nettbank, omfatter dette giro, betalingskort og andre nettbaserte betalingstjenester som telefonbank. Banklovkommisjonen har ikke sett behovet for å vurdere betalingsoverføring ved bruk av sjekk. Slik betalingsoverføring brukes på det nåværende tidspunkt kun i begrenset grad og er ubetydelig i forhold til de andre betalingstjenestene.[1] Overføring ved hjelp av sjekk er dessuten forholdsvis godt regulert, jf. lov av 27. mai 1932 nr. 3 om chekker (sjekkloven).

Dette er fulgt opp i utredningen, slik at betalingsoverføring ved bruk av giro er beskrevet i kapittel 3, betalingsoverføring ved bruk av betalingskort i kapittel 4 og betalingsoverføring ved bruk av nettbaserte betalingstjenester, det vil si særlig nettbank og telefonbank, i kapittel 5. En nærmere beskrivelse av opplegget for utredningen, er for øvrig gitt i avsnitt 1.3 nedenfor.

1.2 Forholdet til betalingstjenestedirektivet

EU vedtok 13. november 2007 et nytt direktiv, R.dir. 2007/64/EF (betalingstjenestedirektivet). I denne forbindelse oppnevnte Finansdepartementet 9. januar 2008 en arbeidsgruppe med utredningsmandat om å foreslå hvordan direktivet skal gjennomføres i norsk rett. I mandatet til arbeidsgruppen er følgende bestemt:

> «13. november 2007 ble det vedtatt nytt direktiv om betalingstjenester i EU, Europaparlaments- og rådsdirektiv 2007/64/EF. Direktivet regulerer harmonisering av markedsadgang og virksomhetsregler for betalingsformidlere som ikke er kredittinstitusjoner, vilkår og regler for betalingsformidlingen og informasjonskrav til tilbyderne av tjenestene, og rettigheter og forpliktelser for brukere og tilbydere av betalingstjenester. Direktivet regulerer dermed både den offentligrettslige og den privatrettslige siden ved betalingstjenester, og vil kreve endringer i norsk regelverk.
>
> Arbeidsgruppen skal foreslå en gjennomføring av EØS-regler som svarer til betalingstjenestedirektivet i norsk rett:
>
> Lov 10. juni 1988 nr. 40 om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven). Kapittel 4a regulerer foretak som har tillatelse til å drive valutavirksomhet, herunder betalingsformidling med utlandet. Disse foretak må ha konsesjon som finansieringsforetak etter lovens § 3-3.

[1] Ca. 500.000 transaksjoner i 2007, jf. Norges Banks årsrapport for betalingssystemer 2007 side 46.

Slike foretak vil bl.a. være underlagt regelverket om ansvarlig kapital. Arbeidsgruppen skal foreslå slike endringer til finansieringsvirksomhetsloven som er nødvendig for å gjennomføre betalingstjenestedirektivet.

Lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag (finansavtaleloven). Loven regulerer i kapittel 2 innskudd og betalingsoppdrag. Arbeidsgruppen skal foreslå nødvendige endringer i finansavtaleloven.

Lov 17. desember 1999 nr. 95 om betalingssystemer m.v. Loven regulerer bl.a. systemer for betalingstjenester basert på standardvilkår for overføring av penger fra eller mellom kundekonti i banker og finansieringsforetak når overføringene bygger på bruk av betalingskort, tallkoder eller annen form for selvstendig brukerlegitimasjon utstedt til en ubestemt krets. Arbeidsgruppen skal vurdere om lovens virksomhetsområde skal utvides til å omfatte de rene betalingsformidlingsforetakene og om loven må endres i samsvar med betalingstjenestedirektivet.

Arbeidsgruppen skal også foreslå endringer i andre lover og forskrifter i den grad dette finnes nødvendig.

Direktivet er i utgangspunktet et fullharmoniseringsdirektiv, men slik at det likevel er gitt flere unntak fra kravet til fullharmonisering. Arbeidsgruppen skal derfor utrede rammen for det handlingsrom direktivet gir ved gjennomføring av bestemmelsene i nasjonal rett, og deretter fremme sitt forslag innenfor denne rammen.

Økonomiske, administrative og andre vesentlige konsekvenser skal utredes i samsvar med utredningsinstruksen kapittel 2.

Utvalget bes avgi sin utredning innen 15. desember 2008.»

I Banklovkommisjonens mandat vedrørende sikkerheten ved blant annet bruk av nettbank, er det sentrale temaet ansvars- og tapsregulering i forholdet mellom kunde og institusjon i tilfeller hvor nettbaserte betalingsoverføringer ikke er blitt gjennomført på riktig måte som følge av feilbruk på kundens side. Finansdepartementet har opplistet tre nærliggende løsningsalternativer for slike oppståtte tapssituasjoner. For det første om finansinstitusjonen kan bli erstatningsansvarlig dersom den tilbyr betalingssystemer med manglende sikkerhet eller lignende. For det andre om kunden har en begrenset tapsrisiko (en egenandel) ved egne feil, det vil si at finansinstitusjonen må dekke tap over et gitt beløp. For det tredje om finansinstitusjonen skal gis en rett til å korrigere feilbetalingen.

En del av disse spørsmålene er til dels regulert i betalingstjenestedirektivet, og vil nødvendigvis inngå i arbeidsgruppens utredning. Verken Finans- eller Justisdepartementet så imidlertid et behov for å endre eller supplere Banklovkommisjonens mandat. I brev av 22. mai fra arbeidsgruppen til Finansdepartementet, uttrykte dessuten gruppen at den ikke kunne se problemer knyttet til avgrensning av gjennomføring av direktivet som et oppdrag, og vurdering av særlige ansvarsregler knyttet til bruk av nettbank mv. *Banklovkommisjonen* har lagt dette til grunn i det videre utredningsarbeidet.

Konsesjonsspørsmål som er angitt i betalingstjenestedirektivet, er det imidlertid lagt opp til at Banklovkommisjonen tar hensyn til i sitt utredningsarbeid vedrørende en samlet lovgivning for finansforetak og finanskonsern (samlet finanslov). I det opplegg til samlet finanslov som har vært og er under arbeid, er konsesjon til betalingsoverføring en av de sentrale konsesjonsformer, og naturlig omfattet av det felles konsesjonssystem basert på EU-/EØS-direktiver som lovutkastet vil inneholde. Betalingstjenestedirektivet artiklene 5 flg. er bygget opp på samme måte som øvrige direktiver på området. Dette ble formidlet til Finansdepartementet i brev av 15. mai 2008 fra Banklovkommisjonen uten at det fremkom innvendinger fra departementet, jf. *brev av 15. august 2008* fra Finansdepartementet. En nærmere redegjørelse av forholdet mellom den foreslåtte ansvarsreguleringen og direktivet er gitt i avsnitt 6.2.3 nedenfor. En oversikt over direktivets bestemmelser er dessuten inntatt som vedlegg 1 til denne utredningen.

Det ble videre, som ledd i denne korrespondansen, dessuten lagt opp til at Banklovkommisjonen også tar for seg andre spørsmål enn kundens egne feil. I brev av 7. mai 2008 fra Justisdepartementet til Finansdepartementet la Justisdepartementet til grunn at dersom Banklovkommisjonen

> «... oppfyller sitt mandat, og finner at den har tid til å utrede også andre spørsmål, har vi heller ikke innvendinger mot at den også ser på andre spørsmål enn kundens egne feil, som for eksempel reglene om andres misbruk av konto mv».

Dette har *Banklovkommisjonen* fulgt opp i det videre utredningsarbeidet. I brev av 15. august 2008 fra Finansdepartementet gis det også uttrykk for at en utredning av tilknyttede spørsmål ikke nødvendiggjør en endring av mandatet. *Banklovkommisjonen* la derfor til grunn at spørsmål vedrørende andres misbruk, kunne inntas i utredningen.

1.3 Opplegget for utredningen

Utredningsarbeidet har – ut fra de ovennevnte avklaringer – vært konsentrert rundt risiko og ansvarsvurderinger knyttet til tapssituasjoner som enten er forårsaket av feilbruk eller misbruk av de aktuelle betalingstjenestene som giro, betalingskort og andre nettbaserte betalingstjenester, særlig nettbank og telefonbank.

Når det gjelder forholdet mellom kunde og institusjon, er Banklovkommisjonens utredning konsentrert rundt spørsmålet om innføring av en ansvarsregulering mellom kunden og institusjonen som tilbyr tjenester innenfor betalingsformidling dersom det forekommer tap som følge av feilbruk eller misbruk. I tråd med forutsetningene i mandatet, har *Banklovkommisjonen* videre vurdert de anførte løsningsalternativene med særlig henblikk på tapssituasjoner som er forårsaket av kundens feilbruk av betalingstjenesten.

Det er særlig de nettbaserte betalingsoverføringene som er utredet nærmere. Hovedfokuset er lagt på nettbank, ettersom denne tjenesten ikke er underlagt klare regler slik som betalingskortene. Den er dessuten, ved siden av nettopp betalingskort, den mest brukte formen for nettbasert betalingsoverføring i dagens transaksjonsbilde. Videre er bruk av telefonbank i flere tilfelle knyttet opp til kundens nettbankkonto. Det finnes likevel visse særegenheter ved telefonbank, og denne betalingsoverføringsformen er derfor også utredet på et selvstendig grunnlag, om enn i et mindre omfang.

I vurderingen av behovet for å innføre en ansvarsregulering ved oppståtte tap som følge av feilbruk eller misbruk, har *Banklovkommisjonen* på den ene siden sett hen til bruksomfanget av de ulike tjenestene, særlig de nettbankbaserte betalingstjenestene, og på den annen side hvilke sikringsmekanismer og tiltak institusjonene selv har iverksatt for å hindre slike tap.

Det er ca. 2,8 millioner nettbankkunder i Norge, noe som tilsvarer 73 prosent av den norske voksne befolkning. I 2007 økte tallet med 300.000.[2] Det er grunn til å anta at omfanget vil fortsette å stige i årene fremover. Driftsikkerheten i nettbankene er i denne sammenheng av stor betydning og vil kunne være avgjørende med tanke på risikoen for at det oppstår tap som følge av feilbruk eller misbruk av nettbanktjenesten. Det kan imidlertid vanskelig tenkes at det ikke vil kunne forekomme tapssituasjoner som er foranlediget av forhold på kundens side. Ved utviklingen av nettbanktjenestenes driftsikkerhet, vil avveiningen mellom sikkerhet og brukervennlighet være viktig. Det er likevel viktig å fremheve at en viss sikkerhet må ligge i bunn. Det er aldri brukervennlig med lav sikkerhet. Brukervennligheten vil først komme inn når en viss sikkerhet er ivaretatt. Dersom systemene av hensyn til sikkerheten gjøres for kompliserte, vil imidlertid tilfanget av kunder kunne reduseres. Det må uansett legges til grunn at sikkerhetstiltak veier tyngre enn ønsket om flest mulig kunder.

Visse tiltak for å øke driftsikkerheten har bankene allerede iverksatt. Det kan i denne sammenheng vises til forslag fra Bankenes Standardiseringskontor, i samråd med Finansnæringens Hovedorganisasjon og Sparebankforeningen, om forbedring av sikkerheten i bankenes nettbankløsninger forfattet i brev av 18. oktober 2006 til Kredittilsynet. Dette er, som antydet foran, tiltak som *Banklovkommisjonen* fortløpende har vurdert betydningen av, særlig i forhold til risikoen for at det oppstår feilbruk fra kundens side, jf. særlig avsnitt 5.4, og det eventuelle dertil foreliggende behovet for en nærmere ansvarsregulering for tap som følge av utilsiktede betalingsoverføringer. Følgende kontrollfunksjoner ble anbefalt fra næringens side for å øke kundenes trygghet i bruk av sine nettbankløsninger:

«1. Feltet for tasting av kontonummer bygges opp med plass til minimum 13 karakterer og det kontrolleres at det tastes inn eksakt 11 siffer. I motsatt fall gis feilmelding.
2. Nettbanken skal ha et kontrollbilde der kunden ser kontonummer, beløp, dato ogeventuell KID eller melding til mottaker i en oversiktlig form.
3. Beløp skal i kontrollbildet fremstå med et klart skille mellom kroner og øre og med bruk av tusenskilletegn.
4. Kunden må aktivt ta stilling til informasjonen i kontrollbildet før vedkommende kan gå videre og betalingen blir iverksatt.
5. Banken kan legge til rette for at kontrollbildet ved et aktivt valg fra kunden ikke framkommer for transaksjoner under en beløpsgrense fastsatt av kunden.
6. I de nettbanker der kunden selv kan styre når kontrollbildet er påkrevd, begrenses dette til beløp under en grense satt av banken.
7. I de nettbanker der det er separate felt for kroner og øre kontrolleres at det kun er tastet inn siffer. Feilmelding fremkommer dersom det er tastet inn noe som helst annet enn siffer i disse feltene.

[2] Sparebankforeningens Nettbankundersøkelse 2008.

8. Dersom nettbanker opererer med ett felt med «kroner, øre» skal kunden fylle inn komma selv om ørebeløpet er 00.
9. Nettbanken har som standard en beløpsgrense pr. transaksjon og/eller for transaksjonsbeløp innen en periode.
10. Grunnet ulik bruk av nettbanken hos kundene bør banken vurdere å la den enkelte kunde selv endre denne beløpsgrensen.
11. I de tilfeller det registreres en transaksjon der mottakers kontonummer ikke finnes i OCR-registeret (KID) og heller ikke er registrert i kundens mottakerregister bes kunden kontrollere at kontonummeret er riktig.
12. Hvis banken gir kunden muligheter til å velge for eksempel beløpsgrense og grense for vising av kontrollbilde, gis kunden en periodisk oversikt av disse valgene.
13. Bankene bør legge til rette for at kunden kan gjennomføre periodisk oppdatering av mottakerregisteret.»

Bankene har så langt *Banklovkommisjonen* kjenner til fulgt samtlige anbefalinger, se også Kredittilsynets rapport av 19. april 2007 om bankenes oppfølging av tiltakene. Som følge av tiltakene, anbefalte Kredittilsynet at det ikke skulle utarbeides en forskrift med hjemmel i betalingssystemloven med generelle regler om nettbanksikkerhet. Forslaget til egenreguleringen ble vurdert som såpass hensiktsmessig at det ikke var behov for nærmere regler på det tidspunkt.

Selv om de ovennevnte kontrollfunksjonene innføres og nye og forbedrede nettbankløsninger utarbeides, har imidlertid *Banklovkommisjonen* vurdert det slik at det alltid vil kunne forekomme feilbruk fra kundens side som kan medføre tap av varierende størrelser. Det at Banklovkommisjonen ble gitt i oppdrag å vurdere behovet for regulering, underbygger også denne oppfatningen. Det vises for øvrig til avsnitt 6.1.3 om det nærmere behovet for en ansvarsregulering for tap som oppstår ved feilbruk eller misbruk.

De løsningsalternativer som er oppført i mandatet, er i utgangspunktet knyttet opp til kundens egne feil. *Banklovkommisjonen* har således, som nevnt foran, vurdert alle tre alternativene i forhold til slike feil, se kapittel 5.4 flg. I forhold til andres misbruk har imidlertid de oppførte alternativene også blitt vurdert som mulige løsninger på potensielle tapssituasjoner som oppstår i slike sammenhenger.

Etter *Banklovkommisjonens* mening bør utgangspunktet være at det økonomiske tapet som enkeltkunder lider, pulveriseres innenfor rammene av de tilbudte betalingstjenestene. Per i dag eksisterer det få klare rettslige holdepunkter vedrørende en nærmere bestemt ansvarsregulering mellom kunde og institusjon for tap som kan oppstå ved bruk av flere av de ulike betalingstjenestene som er tilbudt i markedet. Dette gjelder særlig de nettbaserte betalingstjenester som nettbank og telefonbank. For å kunne vurdere behovet for en nærmere lovregulering, er det blant annet nødvendig å gjennomgå de gjeldende regler for betalingstjenestene som tilbys for bankkunder. Dette er også nødvendig med henblikk på en vurdering av om de gjeldende regler for ulike former for betalingsoverføring bør være gjenstand for en ytterligere detaljregulering. Det er således fortløpende – under de respektive betalingstjenestene – tatt utgangspunkt i gjeldende rett for å vurdere regelbehovet for de enkelte former for betalingstjenester.

I dette arbeidet er det først og fremst tatt utgangspunkt i de nåværende bestemmelser i finansavtaleloven. I kapittel 2 er det gitt en oversikt over disse reglene som danner et godt grunnlag for vurderingen av behovet for ytterligere lovregulering av de aktuelle betalingstjenestene. I kapittel 3 er det redegjort for betalingsoverføring ved giro. En redegjørelse av betalingsoverføring ved hjelp av betalingskort, både debet- og kredittkort, er gitt i kapittel 4. I kapittel 5 er det videre redegjort for overføring ved hjelp av andre nettbaserte betalingstjenester som telefonbank og nettbank. I forhold til de nettbaserte betalingstjenestene er det også sett hen til regler i kontoavtalen og avtalevilkår mellom kunden og institusjonen, andre aktuelle lovbestemmelser på området, samt alminnelige erstatningsregler.

1.4 Banklovkommisjonens arbeid

Frist for avgivelse av utredningen ble i første omgang satt til 31. desember 2007, jf. brev av 13. mars 2007 fra Finansdepartementet. Banklovkommisjonen fikk imidlertid kort tid etter dette mandatet, i oppdrag å utarbeide utkast til lovgivning om skattebegunstiget individuell pensjonsordning i samsvar med pensjonsforliket i Innst. S. nr. 168 (2006-2007), avgitt på grunnlag av Revidert Nasjonalbudsjett i St.meld. nr. 5 (2006-2007), jf. brev fra Finansdepartementet av 15. mai 2007. Forutsetningen fra Stortinget var at den nye lovgivningen kunne vedtas i 2008 med virkning for skatteåret 2008. Frist for utredningen ble satt til februar 2008. Utredningen om individuell pensjonsordning ble således prioritert av Banklovkommisjonen.

Arbeidet viste seg å være en tidkrevende og arbeidskrevende oppgave i forhold til den samlede

utredningskapasitet i Banklovkommisjonen, og arbeidet med utredningen om nettbankbasert betalingsoverføring måtte stilles i bero. Banklovkommisjonen søkte på dette grunnlag, i brev av 16. oktober 2007, om forlengelse av dette arbeidet til 1. juli 2008. I brev av 16. november 2007 utsatte Finansdepartementet fristen for avgivelse av utredningen til 1. juli 2008.

Etter ferdigstillelsen av Banklovkommisjonens utredning om individuelle pensjonsordninger i desember 2007, startet Banklovkommisjonen arbeidet med en utredning om nettbankbasert betalingsoverføring. I brev av 29. april 2008 fra Finansdepartementet fikk imidlertid Banklovkommisjonen i oppdrag å utarbeide utkast til de endringer i finansieringsvirksomhetsloven §§ 2-2 følgende som var påkrevd ved gjennomføringen av direktiv 2007/44/EF i finanslovgivningen. I mandatet ba Finansdepartementet om at Banklovkommisjonens utkast ble ferdigstilt innen 15. september 2008. Banklovkommisjonen måtte derfor prioritere dette arbeidet. Utredningen ble avgitt 6. august 2008 til Finansdepartementet. Banklovkommisjonen kunne således ikke sluttføre utredningsarbeidet vedrørende nettbankbasert betalingsoverføring innen den utsatte fristen. I brev av 15. august 2008 fra Finansdepartementet ble det lagt til grunn at utredningsarbeidet i stedet skulle sluttføres så snart som mulig. Ved siden av det videre arbeidet med en utredning om spørsmål knyttet til sikkerheten ved bruk av blant annet nettbank, har Banklovkommisjonen avsluttet arbeidet med en utredning om skadeforsikringsselskapenes virksomhet, avgitt som NOU 2008: 20 Skadeforsikringsselskapenes virksomhet. I brev av 20. juni 2008 fra Finansdepartementet ble Banklovkommisjonen dessuten gitt i oppdrag å utrede regler knyttet til sparebanker og egenkapital. Dette arbeidet har også foregått parallelt med utredningen om nettbankbasert betalingsoverføring.

Del II
Ansvarsregulering og risikoaspekter ved bruk av betalingsinstrumenter

Kapittel 2
Finansavtalelovens regler om bankkonto

2.1 Innledning

Lov om finansavtaler og finansoppdrag av 25. juni 1999 nr. 46 (finansavtaleloven) gjelder for avtaler og oppdrag om finansielle tjenester med finansinstitusjoner. Den er basert på forslag fra Banklovkommisjonen som ble gitt i kommisjonens første utredning (NOU 1994: 19 Finansavtaler og finansoppdrag). Justisdepartementet fulgte i all vesentlighet opp forslaget, jf. Ot.prp. nr. 41 (1998-99) Om lov om finansavtaler og finansoppdrag. Finansavtaleloven var et viktig skritt i retning av et sterkere og bedre forbrukervern ved bruk av betalingstjenester. Behovet for forbrukervern var på dette tidspunktet således et viktig tema for Banklovkommisjonen og ble tillagt vesentlig vekt ved utforming av forslag til lovbestemmelsene. Hovedhensynene bak Banklovkommisjonens forslag – som også ble fulgt opp av departementet – var å bidra til, og å skape, en klarere og mer oversiktlig rettstilstand, balanserte kontraktsvilkår for kundene og en effektiv konkurranse.

Banklovkommisjonen er nå gitt i oppdrag å utrede spørsmål i tilknytning til risiko, behov for ansvarsregulering og det eventuelt nærmere innholdet av en ansvarsregulering for tap som oppstår som følge av feilbruk eller misbruk av de ulike betalingstjenester. De betalingstjenestene som benyttes mest i våre dager er giro, betalingskort, telefonbank og nettbank. Dette er tjenester som i all hovedsak er knyttet opp mot en innskuddskonto og er omfattet av finansavtalelovens kapittel 2 om innskudd og betalingsoppdrag, jf. lovens § 9 første ledd og avsnittet nedenfor. For å vurdere lovgivningsbehovet når det gjelder de aktuelle betalingstjenestene, herunder nettbank og telefonbank, har Banklovkommisjonen derfor først og fremst tatt utgangspunkt i reglene som er fastslått i denne loven.

Det er mange potensielle tapssituasjoner som kan oppstå ved en kundes bruk av betalingstjenester. Dette henspeiler seg i første rekke på kundens bruk av kontoen, samt risikoen for feilbelastninger og misbruk fra uvedkommende. Den videre drøftelsen er knyttet opp mot denne inndelingen. Først gjennomgås imidlertid finansavtalelovens regler om avtaleinngåelse mellom kunde og institusjon. Denne avtalen legger til rette for kundens bruk av konto, herunder betalingsoverføring, og er således et forhold som bør beskrives. Det kan videre ikke utelukkes at forhold under avtaleinngåelsen kan lede til økonomisk tap for en kunde, for eksempel som følge av identitetstyveri mv.

Selv om Banklovkommisjonen tar utgangspunkt i finansavtaleloven, er det viktig å merke seg at også andre lovbestemmelser kan være aktuelle. Disse vedrører likevel mer spesifikke områder og er således isteden – så langt de er aktuelle – inntatt under redegjørelsen av de enkelte betalingstjenestene i kapittel 3, 4 og 5.

Som nevnt foran er det først og fremst kapittel 2 om innskudd og betalingsoppdrag i finansavtaleloven som er aktuelt i forhold til betalingstjenestene. I henhold til lovens § 9 første ledd gjelder dette kapitlet for avtaler om innskudd og for bruk av innskuddskonto i finansinstitusjoner. De fleste betalingsoverføringer er knyttet opp mot kundens bankkonto. Dette gjelder imidlertid ikke ubetinget, som for eksempel ved forhåndsbetalte elektroniske kort. Slike oppdrag er ikke omfattet av bestemmelsene i kapitlet, jf. § 11, og er heller ikke tema for den videre utredningen. Forholdet mellom betaler og mottaker ved betalingsoverføringer i finansavtaleloven kapittel 2 VI er for øvrig også utelatt.

I den videre redegjørelsen av henholdsvis avtaleinngåelse, bruk av konto, feilbelastning og andres misbruk, er det tatt utgangspunkt i Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) og Ot.prp. nr. 41 (1998-99) Om lov om finansavtaler og finansoppdrag, så langt innholdet i disse dokumentene er forenlig. Det er således Odelstingsproposisjonen som er brukt som referansepunkt i beskrivelsen av de gjeldende bestemmelsene. Det er for så vidt gjort visse nødvendige oppdateringer og bemerkninger for å tilpasse innholdet til og reflektere utviklingen av de aktuelle betalingsinstrumentene.

2.2 Avtaleinngåelse

For å kunne foreta betalingsoverføringer – enten via giro, betalingskort, nettbank eller telefonbank – må det inngås en avtale mellom institusjonen og kunden. Dette kalles for en kontoavtale. I avtalen fremgår det hvilke regler og vilkår som gjelder for innskudd og betalingsoppdrag, enten i hovedavtalen eller som vedlegg til avtalen. Vilkårene skal holdes tilgjengelig for kundene på ekspedisjonsstedene, jf. § 13 første ledd. Disse vilkårene er som oftest også nå tilgjengelige på institusjonens nettsteder.

Før kunden velger å inngå en kontoavtale med institusjonen, må kunden bestemme seg for hva slags innskuddskonto han eller hun vil benytte seg av. Etter lovens § 15 første ledd er det bestemt at institusjonen skal veilede kunden i dette valget. Dette innebærer at kunden bedre skal settes i stand til å velge riktig kontotype. Hvilke innskuddskonti som institusjonen skal opplyse om, vil først og fremst være avhengig av hvilke behov vedkommende kunde må antas å ha på bakgrunn av de opplysninger institusjonen får fra kunden. Finansavtaleloven § 15 annet ledd bestemmer videre at institusjonen skriftlig skal opplyse om en rekke andre forhold, blant annet regler om hvordan kontoen og betalingsinstrumentet kan brukes og kravene til legitimasjon, jf. bokstav d). Etter bestemmelsens bokstav g) skal det også opplyses om ansvar og risiko ved bruk av kontoen og for andres urettmessige bruk av den. Kravet om skriftlighet gjelder, jf. § 16 første ledd, men avtalen kan inngås i elektronisk form dersom kunden ønsker dette, jf. § 8 første ledd. Slike opplysninger skal – på samme vis som med alminnelig vilkår – også være lett tilgjengelige for alle kunder, jf. § 15 tredje ledd.

Dersom avtalen skal inngås i elektronisk form, stilles det krav om at avtalens innhold i sin helhet er tilgjengelig ved avtaleinngåelsen, jf. lovens § 8 annet ledd bokstav a). På samme måte som ved en ordinær papirbasert avtaleinngåelse, bør kunden ha mulighet til å sette seg inn i alle avtalevilkårene før han eller hun binder seg til avtalen, jf. Ot.prp. nr. 41 (1998-99) side 95. I tillegg må det være benyttet en betryggende metode for å autentifisere inngåelsen av en avtale med det angitte innhold, jf. §8 annet ledd bokstav b). I forarbeidene – Ot.prp. nr. 41 (1998-99) side 26 – er det fastslått at kravet om betryggende metode innebærer at metoden må være egnet til å identifisere avsenderen av meldinger i forbindelse med avtaleinngåelse, å vise at meldingen er sendt i den hensikt å foreta en rettslig disposisjon, samt å sikre bevis i tilfelle en senere konflikt om avtalens eksistens og innhold. Vurderingen av om en metode er betryggende, vil variere ut fra den foreliggende teknologien på det tidspunkt avtalen inngås og ut fra hva som er innholdet i den avtalen som inngås. Departementet antok for eksempel at bruk av PIN-kode eller lignende, vil kunne anses som en betryggende metode for å inngå en avtale om mindre endringer i innskuddsvilkår. På den annen side må det, etter departementets oppfatning, være klart at dersom en låneavtale med en forbruker inngås elektronisk, vil det bare kunne skje gjennom et system med elektronisk signatur eller en annen metode som gir tilsvarende sikkerhet.

Avtalen skal videre inneholde navn og adresse samt fødselsnummer på kontohaveren og enhver som skal disponere kontoen, jf. § 16 første ledd annet punktum. Den skal også inneholde opplysninger som er nevnt i finansavtaleloven § 15 annet ledd bokstav a) til i). Vilkår som ikke er tatt inn i kontoavtalen, er ikke bindende for kontohaveren med mindre institusjonen godtgjør at vilkåret er vedtatt av kontohaveren, jf. § 16 tredje ledd. Det klare utgangspunkt vil uansett være at et vilkår må være tatt inn i selve avtalen for at det skal være bindende for kunden, jf. Ot.prp. nr. 41 (1998-99) side 100.

På bakgrunn av vilkårene som er oppstilt i finansavtaleloven, har næringens bransjeorganisasjoner utarbeidet standardiserte vilkår for innskudd og betalingsoppdrag.[1] Visse standardiserte regler tilknyttet nettbanktransaksjoner er også utarbeidet, men her har de enkelte bankinstitusjonene større variasjoner enn for de alminnelige vilkår for innskudd og tradisjonelle betalingsoppdrag. Dette er nærmere belyst i avsnittene 5.5.2 og 6.3.2 nedenfor.

I finansavtaleloven § 18 er det gitt regler om endring av kontoavtalen. Såframt partene er enige om å endre avtalen, gjelder reglene i §§ 15 og 16 tilsvarende så langt de passer, jf. § 18 første ledd. Institusjonen kan som utgangspunkt ikke ensidig endre avtalevilkår til skade for kontohaveren. Dette gjelder imidlertid ikke for nedsettelse av rentesats og økning av gebyrer for å ha eller bruke kontoen eller betalingsinstrument knyttet til denne, jf. § 18 annet ledd bokstav a) og b). Begrunnelsen var her at institusjonene til enhver tid bør kunne tilpasse sine innlånskostnader til det gjeldende rentenivå, samt at offentligrettslige krav til betalingstjenestens innretning vil kunne representere betydelige kostnadsøkninger som institusjonen ikke har herredømme over, jf. Banklovkommi-

[1] Utarbeidet av Sparebankforeningen og Finansnæringens Hovedorganisasjon.

sjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 118. Videre kan institusjonen endre satsene for overtrekksrente og purregebyr ved urettmessig overtrekk, jf. § 18 tredje ledd.

Ensidig endring av avtalevilkårene krever imidlertid varsel. I finansavtaleloven § 19 første ledd er det bestemt at slik endring tidligst kan settes i verk to uker etter at institusjonen har sendt skriftlig varsel til kontohaveren om endringen. Skriftlighetskravet er også her oppfylt ved bruk av elektroniske medier dersom kunden ønsker dette, jf. lovens § 8 første ledd.

Avtale om belastningsfullmakt er underlagt særskilte regler og er redegjort for i avsnitt 2.3.3 nedenfor, ettersom det hører til kundens bruk av konto.

2.3 Bruk av konto

2.3.1 Generell bruk og oversikt

Innskuddskontoen danner utgangspunktet for ulike typer av tjenester. I henhold til finansavtaleloven § 24 første ledd kan kontohaveren bruke kontoen til innskudd, uttak og betalingsoverføringer i samsvar med kontoavtalen. Rettslig sett har bestemmelsen liten selvstendig mening. For å finne ut hva den enkelte konto kan brukes til, må det søkes i den enkelte kontoavtale. I avtalen kan det for så vidt bestemmes at anvendelsesområdet for en konto skal være snevrere eller bredere enn det som er angitt i første ledd, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 123.

Etter lovens § 24 annet ledd er det gitt visse regler for når lønnskonto, driftskonto og lignende brukskonto kan disponeres av kontohaveren. Hovedregelen etter bestemmelsens første punktum er at disponering av innskudd på slik konto kan foretas når innskuddet er godskrevet kontoen. Ved betalingsoverføring vil det kunne ta en viss tid fra betalingsoppdrag inngis og til betalingsmottakerens konto godskrives. Dette har blant annet sammenheng med at kontroll- og bokføringsrutiner i henholdsvis betalers og mottakers bankinstitusjon kan ta en viss tid. En nærmere gjennomgang av avregningene bankene imellom, er gitt i avsnitt 6.2.4 nedenfor. De alminnelige vilkår skal for så vidt opplyse om høyeste antall virkedager for å gjennomføre betalingsoppdrag, jf. finansavtaleloven § 13 annet ledd.

Etter lovens § 24 annet ledd annet punktum er hovedregelen om tidspunkt for disponering modifisert. Uavhengig av fra hvilket tidspunkt innskuddet godskrives kontoen, kan innskuddet straks heves på institusjonens ekspedisjonssteder. Dette gjelder bare i forhold til betjente ekspedisjonssteder som har mulighet til å kontrollere at beløpet faktisk er satt inn på kontoen, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 123.

Institusjonen skal jevnlig, og minst én gang årlig, skriftlig informere kunden om rente- og gebyrsatser for alternative typer innskuddskontoer som institusjonen tilbyr, jf. finansavtaleloven § 30 første ledd. Institusjonen bestemmer selv tidspunktet for slik utsendelse, men meningen er at det i alle fall ikke skal gå mer enn ett år mellom hver slik utsendelse. Slike opplysninger kan gis ved hjelp av elektronisk kommunikasjon dersom kunden ønsker dette, jf. finansavtaleloven § 8 første ledd. Etter lovens § 30 annet ledd første punktum skal kontoutskrift sendes kontohaveren etter årets utgang. Utskriften representerer et viktig kontrollinstrument både for kontohaveren og institusjonen. For kontohaveren vil kontoutskriften ofte være avgjørende for at denne skal kunne holde seg orientert om inn- og utbetalinger på kontoen. Utskriften gjør det mulig for kontohaveren å holde oversikt over egen økonomi, samt kontrollere at det ikke har forekommet utilsiktede eller urettmessige belastninger. Den gir således mulighet til å oppdage eventuelle feil eller uregelmessigheter og er en forutsetning for at kontohaveren skal kunne være i stand til å melde fra om feil til institusjonen. Reglene om kontoinformasjon ivaretar på denne måten både et opplysningsbehov og representerer en viktig kontrollfunksjon.

For lønnskonto og driftskonto vil ikke målet med at kontohaveren skal kunne holde oversikt over egen økonomi og kunne kontrollere belastningene på kontoen oppfylles dersom kontoutskrift bare blir sendt én gang i året. Etter lovens § 30 annet ledd annet punktum er det derfor bestemt at kontoutskrift for lønnskonto, driftskonto og lignende konto skal sendes hver måned. Denne plikten gjelder imidlertid bare dersom det har vært bevegelse på kontoen.

For nettbanktjenester er dette løst ved at kunden har forholdsvis god oversikt over sine transaksjoner til enhver tid, noe som også må anses hensiktsmessig og nødvendig tatt i betraktning det store og økende antall nettbanktransaksjoner, jf. avsnitt 5.2.1. Dette gjelder som regel uavhengig av om kunden har knyttet nettbanktjenesten opp mot en brukskonto eller lignende.

Hver kontoutskrift skal inneholde saldo, alle bevegelser på kontoen siden forrige utskrift, tids-

punkter for renteberegninger for de enkelte bevegelser, gebyrer siden forrige utskrift og samlet fra siste årsskifte, påløpte renter og de rente- og gebyrsatser som gjelder for kontoforholdet, jf. finansavtaleloven § 30 tredje ledd. Bestemmelsen er ikke til hinder for at det gis ytterligere opplysninger på kontoutskriftene om dette skulle være ønskelig. I tillegg til alle bevegelsene skal også valuteringstidspunkt for de enkelte betalingsoverføringer fremgå.

For å lette kontohaverens kontroll med kontoutskriftens riktighet, skal det i tilknytning til de enkelte bevegelser være oppgitt navn på betalingsmottakere og betalere. Bestemmelsen i tredje ledd annet punktum pålegger institusjonen å innta navn på betalingsmottakere så langt som mulig. Dette er også et viktig moment i forhold til kundens mulighet til å holde oversikt og kontroll over belastninger som gjøres på vedkommendes konto.

Dersom kontohaveren har fått uriktige opplysninger om innestående og vedkommende i god tro har belastet kontoen, kan dette føre til at kontohaveren i ren villfarelse belaster kontoen for mer enn disponibelt beløp. Dette gjelder uansett om opplysningene er fremkommet på kontoutskrift, ved kontofon eller fra institusjonen på annen måte, for eksempel ved kontoutskrift over nettbank. I disse tilfellene er det fastslått at institusjonen ikke kan kreve overtrekksrente av kontohaveren før kontohaveren har fått rimelig tid til å rette forholdet, jf. finansavtaleloven § 30 fjerde ledd. I tråd med alminnelige rettsprinsipper kreves det at den gode tro er aktsom. Dersom den feilaktige godskrivingen er av betydelig størrelse og kontohaveren burde forstått at det forelå en feil, vil vilkårene i bestemmelsen ikke være oppfylt, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 141.

2.3.2 Tid og sted for betaling

Finansavtalelovens regler om tid og sted for betaling i § 39 er sentrale i forhold til blant annet kundens mulighet til å tilbakekalle et betalingsoppdrag. Dette er i sin tur et viktig spørsmål i de tilfeller hvor kunden selv oppdager at det er gjort en feil og ønsker å tilbakekalle oppdraget. Dette vil kunne redusere risikoen for at kunden påføres et tap. Dersom kunden har gjort en feil og iverksatt en transaksjon, har det imidlertid formodningen mot seg at kunden vil oppdage dette i tide, for eksempel vil jo en etterfølgende kontoutskrift kunne gjøre kunden oppmerksom på dette, noe som kan komme opptil en måned etter den gjennomførte transaksjonen, jf. avsnitt 2.3.1 foran. Tilbakekall av betalingsoppdrag gjennomgås i avsnitt 2.5 nedenfor. I det følgende gis en kort beskrivelse av reglene om tid og sted for betaling. De regler som knytter seg til betaling i kontanter er utelatt.

Når det gjelder betalingstiden, henger dette først og fremst sammen med når mottakeren ikke lenger skal kunne gjøre gjeldende misligholdssanksjoner på grunn av forsinkelse, det vil si når oppgjøret virker fristavbrytende. Dernest er temaet knyttet til når en betaling er frigjørende. Med dette menes at betaleren er fri sin betalingsforpliktelse, og at mottakeren ikke lenger kan kreve oppfyllelse av betaleren selv om beløpet ikke skulle ha kommet frem til mottakeren.

I finansavtaloven § 39 er følgende bestemmelse fastslått:

«**§ 39.** *Tid og sted for betaling*

(1) Dersom betaleren har rett til å foreta oppgjør ved overføring til mottakerens konto, anses betalingen for å være skjedd når beløpet er godskrevet mottakerens institusjon. Ved overføring innen samme institusjon anses betaling for å være skjedd når beløpet er godskrevet mottakerens konto. Når oppgjør skal skje ved utbetaling i kontanter, anses betalingen for å ha skjedd når beløpet er stilt til mottakerens disposisjon gjennom bank på mottakerens sted og melding om dette er kommet frem til mottakeren.

(2) Dersom ikke annet er avtalt, anses dessuten en fastsatt betalingsfrist for å være avbrutt

a) ved betaling fra forbruker når betalerens oppdrag er mottatt av enfinansinstitusjon
b) når mottakeren mottar og aksepterer sjekk eller annet betalingsmiddel.

(3) Dersom et mottatt betalingsoppdrag ikke skal utføres straks, regnes avbruddet av betalingsfristen fra den avtalte betalingsdagen.

(4) Betalingsfristen avbrytes ikke dersom betalingsoppdraget ikke blir gjennomført og dette skyldes betalerens eget forhold. Institusjonen skal i så fall varsle betaleren om dette uten ugrunnet opphold, med mindre annet er bestemt i eller i medhold av lov.»

Første ledd første punktum gjelder tidspunktet for betaling i tilfeller der betaleren har rett til å foreta oppgjør ved betaling til mottakerens konto. Betaling skal anses å være skjedd når beløpet er godskrevet mottakerens institusjon og er i samsvar med bestemmelsen i R.dir. 2007/64/EF artikkel 64 om kvittering for betalingsoppdrag. Annet punktum inneholder en særlig regel for overføring innen samme institusjon. I slike tilfeller skal betaling anses for å være skjedd når beløpet er godskrevet mottakerens konto.

Når betaleren er en forbruker, følger det av annet ledd bokstav a) at betalingsfristen, dersom ikke annet er avtalt, anses for å være avbrutt når betalerens oppdrag er mottatt av en finansinstitusjon. Begrepet «mottatt» vil normalt være identisk med første innlevering eller registrering hos institusjonen. Ved innlevering av oppdrag over skranke, vil en normalt få kvittering for at oppdraget er mottatt. For papirbaserte girotjenester som ikke leveres i skranke, er det vanligvis tilrettelagt systemer for mottak, for eksempel gjennom girokasser plassert i ekspedisjonens lokaler eller bruk av brevgiro som sendes BBS direkte. Oppdraget er i disse tilfellene mottatt når det er lagt i girokassen eller det er kommet frem til BBS. For nettbanktjenestene vil avbrudd av betalingsfrist for regninger som skal belastes samme dagen, anses å ha skjedd idet kunden har samtykket i transaksjonen og den er sendt til forfallsregisteret. Dette må anses som at oppdraget er innlevert eller registrert hos institusjonen. De spørsmål som melder seg i forhold til tilbakekall er drøftet i avsnitt 2.5 nedenfor.

Etter annet ledd bokstav b) anses en fastsatt betalingsfrist som avbrutt når mottakeren mottar og aksepterer sjekk eller annet betalingsinstrument. Annet betalingsinstrument vil kunne være giro, betalingskort eller annet særskilt hjelpemiddel for overføring av betalingsmidler, jf. finansavtaleloven § 12 bokstav c).

Etter tredje ledd regnes avbruddet av betalingsfristen fra den avtalte betalingsdagen dersom et mottatt betalingsoppdrag ikke skal utføres straks.

Dersom et betalingsoppdrag ikke gjennomføres og årsaken til dette skyldes betalerens eget forhold, avbrytes ikke betalingsfristen, jf. fjerde ledd første punktum. Regelen ble forutsatt å være aktuell dersom det for eksempel ikke er dekning på betalerens konto, eller at betaleren har gitt feil eller ufullstendige opplysninger om hvem som er mottaker. I annet punktum er det bestemt at institusjonen i så fall skal varsle betaleren uten ugrunnet opphold med mindre annet er bestemt i eller i medhold av lov.

2.3.3 Belastningsfullmakt

De fleste finansinstitusjoner tilbyr mer omfattende og sammensatte betalingstjenester enn utføring av enkeltstående betalingsoppdrag. I forhold til slike mer omfattende tjenester kan det sondres mellom avtaler om faste betalingsoppdrag og avtaler om direkte debitering.

En avtale om faste betalingsoppdrag går ut på at institusjonen skal betale én eller flere regninger for kontohaveren, for eksempel strøm- og telefonregninger. Oppdraget kan være løpende eller tidsbegrenset. Faste betalingsoppdrag innebærer et fullmaktsforhold mellom kontohaveren og finansinstitusjonen. Det er i dag ingen lovfestede begrensninger i hva fullmakten kan inneholde eller krav til hva den skal inneholde.

En ordning med direkte debitering gir betalingsmottakeren (kreditor) muligheten til å belaste betalerens (debitors) konto ved forfall. Skal tjenesten være praktisk, bør betaleren og mottakeren ha et fast forretningsforhold der det jevnlig foretas betalingsoverføringer. Fordelen med direkte debitering er at betaleren slipper å kontakte banken for at regningene skal bli betalt ved forfall. Ulempen er at betaleren kan miste oversikten og kontrollen over belastningene på kontoen, noe som øker med mengden av regningene som betales gjennom slik belastningsform. I dag tilbyr bankene i første rekke to former for direkte debitering: Autogiro og Avtalegiro, dog slik at førstnevnte tjeneste ikke lenger tilbys forbrukerkunder.

Slik Autogiro er oppbygd, inngås det først en avtale mellom mottakeren og mottakerens bankforbindelse. Deretter innhenter mottakeren en belastningsfullmakt fra betaleren. Det er mottakeren – eller dennes bankforbindelse – som sender betalers bank informasjon om den fullmakten betaleren har gitt. Fullmakten registreres på betalerens konto. På forfallsdagen belastes så betalerens konto etter initiativ fra betalingsmottakeren eller hans institusjon.

Avtalegiro er bygd opp på en annen måte enn Autogiro. Bruk av Avtalegiro forutsetter at betaleren og betalingsmottakeren har inngått generelle avtaler med sine institusjoner om at betalinger kan skje gjennom denne ordningen. Den konkrete debiteringsordningen mellom partene kommer i stand ved at betaleren, på eget initiativ eller på oppfordring fra mottakeren, gir sin institusjon fullmakt til å etterkomme debiteringskrav fra mottakeren. Institusjonen sender så melding om dette til mottakeren og hans institusjon.

I forarbeidene fremkommer det klart at det er viktig å ha klare lovregler om faste betalingsoppdrag og direkte debitering. *Banklovkommisjonen* anså på generelt grunnlag flere faremomenter tilknyttet slike belastninger, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 76. Det ble derfor foreslått visse regler for at slike belastninger skulle skje i mer betryggende former. Departementet støttet dette synspunktet, særlig som følge av faren for kreditors mulighet til å foreta belastninger uten debitors samtykke slik at sistnevnte kunne miste

oversikten, jf. Ot.prp. nr. 41 (1998-1999) side 32 og 33. Det ble imidlertid foretatt visse endringer i lovteksten som nå er inntatt i finansavtaleloven § 26. Denne fastslår følgende:

«**§ 26.** *Avtale om belastningsfullmakt*

(1) Denne bestemmelsen gjelder for

a) avtale mellom kontohaveren og institusjonen om fast betalingsoppdrag der belastning skal kunne skje etter krav fra betalingsmottakeren eller foretas av institusjonen av eget tiltak

b) avtale mellom kontohaveren og betalingsmottakeren om at kontoen gjentatte ganger skal kunne belastes etter krav fra betalingsmottakeren.

(2) Kontohaveren skal gi institusjonen skriftlig melding om avtale som nevnt i første ledd bokstav b.

(3) Institusjonen skal påse at de belastninger som foretas, ligger innenfor avtalens grenser.

(4) Avtalen skal på en entydig måte identifisere betalingsmottakeren. For hver betalingsmottaker skal avtalen angi en høyeste belastningsgrense og det tidsrommet belastningsgrensen knytter seg til.

(5) Dersom ikke annet er uttrykkelig avtalt, skal institusjonen sørge for at varsel sendes til kontohaveren senest sju virkedager før belastningen finner sted. Varslet skal opplyse om tidspunktet for når belastningen vil finne sted, om betalingsmottakeren og om beløpets størrelse. Varslet kan tas med i kontoutskrift som nevnt i § 30 annet ledd annet punktum.

(6) Kontohaveren kan endre eller tilbakekalle fullmakten ved melding til institusjonen. Institusjonen skal gjennomføre endringen eller tilbakekallet senest første virkedag etter at meldingen er kommet fram.»

Bestemmelsens første ledd presiserer virkeområdet for bestemmelsen. Bestemmelsens første ledd bokstav a) gjelder der kontohaveren og institusjonen inngår avtale om at institusjonen skal gjennomføre et fast betalingsoppdrag. Avtalen kan gå ut på at institusjonen av eget tiltak skal foreta betaling på et bestemt tidspunkt eller at betaling skal skje etter krav fra betalingsmottakeren. Dette vil blant annet omfatte ordinære faste betalingsoppdrag og avtaler om bruk av tjenesten Avtalegiro, jf. Ot.prp. nr. 41 (1998-1999) side 103. Første ledd bokstav b) gjelder der det inngås avtale mellom kontohaveren og betalingsmottakeren om at kontoen gjentatte ganger skal kunne belastes etter krav fra betalingsmottakeren. Dette vil blant annet omfatte avtaler innenfor tjenesten Autogiro. Kravet om skriftlighet er ikke til hinder for at melding gis ved hjelp av elektronisk kommunikasjon, jf. finansavtaleloven § 8 første ledd.

2.4 Feilbelastninger

I finansavtaleloven er det gitt regler om både feilaktig godskriving og feilaktig belastning av konto. De førstnevnte situasjonene er ikke like aktuelle for denne utredningens tema og vurderingsgrunnlag, ettersom det her ikke forekommer et tap for kunden. Dette er således utelatt i den videre fremstillingen. Feilbelastninger av en kundes konto er først og fremst regulert i finansavtaleloven § 32. I lovens § 33 er det videre gitt visse regler om frist for melding av slike feil. Dette omtales til slutt i dette avsnittet.

Etter finansavtaleloven § 32 er følgende bestemt:

«**§ 32.** *Feilaktig belastning av konto*

(1) Hvis institusjonen ved en feil har belastet en konto, skal den uten ugrunnet opphold godskrive kontoen for et tilsvarende beløp.

(2) Institusjonen plikter uten hensyn til skyld å erstatte rentetap og annet direkte tap som er oppstått ved den feilaktige belastningen.

(3) For indirekte tap svarer institusjonen etter alminnelige erstatningsregler.»

Hvis institusjonen ved en feil har belastet en innskuddskonto, skal den uten ugrunnet opphold godskrive kontoen med et tilsvarende beløp. Dette er inntatt i første ledd. Plikten til å tilbakeføre et tilsvarende beløp uten ugrunnet opphold gjelder uansett om institusjonen selv oppdager den feilaktige belastning, eller først blir klar over forholdet etter henvendelse fra kontohaverens side.

Regelen om feilaktig belastning av konto gjelder i de tilfeller hvor det er en feil fra institusjonen selv som har medført belastningen. Når den feilaktige belastning er initiert av andre enn institusjonen eller dens medhjelpere, gjelder bestemmelsene i finansavtalelovens kapittel 2 V om andres misbruk av konto og betalingsinstrument, se nedenfor avsnitt 2.6.

I motsetning til reglene om feilaktig godskriving av konto, inneholder ikke § 32 noen tidsfrist for når retting av feilen må skje. Departementet bemerket at kravet om tilbakeføring neppe kan anses som noen selvstendig fordring som vil være gjenstand for foreldelse. Den egentlige fordringen vil være kundens krav på utbetaling av innestående beløp på kontoen. Dermed vil regelen om 20 års foreldelse for bankinnskudd i foreldelsesloven § 4

gjelde selv om deler av innskuddet er «tatt ut» av kontoen gjennom en feilaktig belastning.

Bestemmelsen i første ledd om institusjonens plikt til å tilbakeføre beløp som er belastet ved en feil, innebærer at institusjonen i kontoavtale ikke kan innføre regler om at kontohaveren må reklamere innen en viss frist for ikke å forspille retten til å kreve tilbakeføring av beløpet. I tillegg til å tilbakeføre et tilsvarende beløp, er institusjonen etter annet ledd forpliktet til å erstatte rentetap og annet direkte tap som har oppstått ved den feilaktige belastning. Det antas at det i de fleste tilfeller vil være mest praktisk å yte erstatning i form av tilbakevalutering.

Etter tredje ledd svarer institusjonen også for indirekte tap etter alminnelige erstatningsregler. Dette innebærer at erstatningsansvaret vil være avhengig av at belastningen har skjedd ved uaktsomhet eller forsett, at kontohaveren har lidt økonomisk tap og at det foreligger årsakssammenheng mellom institusjonens handling og tap. For konsekvenstap vil det for eksempel måtte kreves at kontohaverens tap var en påregnelig følge av institusjonens handling. Videre vil alminnelige regler om arbeidsgiveransvar, om lempning av ansvar og om læren om anonyme og kumulative feil komme til anvendelse. Banklovkommisjonen går imidlertid ikke nærmere inn på dette.

I finansavtaloven § 33 er institusjonen forpliktet til å melde om uregelmessigheter i forhold til både godskriving og belastning av en kundes konto. Den fastslår følgende:

«**§ 33.** *Melding om feil*
Oppdager institusjonen at en konto er feilaktig godskrevet eller belastet, skal kontohaveren underrettes uten ugrunnet opphold. Dersom feilen er rettet på en slik måte at det ikke er noen reell mulighet for at kontohaveren kan ha fått uriktige opplysninger om disponibelt beløp på kontoen, er det likevel tilstrekkelig at underretningen gis i forbindelse med en kontoutskrift.»

I forarbeidene ble det fastslått at det er viktig at kontohaveren så snart som mulig får beskjed dersom kontoen blir godskrevet eller belastet ved en feil. Dette har sammenheng med at kontohaveren gjennom kontoutskrifter eller ved forespørsel om saldo kan ha fått oppgitt feil saldo og innrettet seg etter dette. I bestemmelsens første punktum er det derfor fastslått at kontohaveren skal gis melding om forholdet uten ugrunnet opphold. Departementet fant det videre ikke nødvendig at umiddelbar varsling skulle gis dersom det ikke er noen reell mulighet for at kunden kan ha fått uriktige opplysninger om innestående på kontoen. I slike tilfeller ble det ansett som tilstrekkelig at varsling skjer i forbindelse med ordinær kontoutskrift, jf. annet punktum.

Om virkningene av overtrekk når kontohaveren har fått uriktige opplysninger om innestående på konto, vises det til avsnitt 2.3.1 foran om finansavtaleloven § 30 fjerde ledd.

2.5 Tilbakekall av betalingsoppdrag

Av og til vil det kunne være behov for å tilbakekalle eller endre et betalingsoppdrag. Grunnen til dette kan for eksempel være at betaleren er blitt oppmerksom på at betalingsmottakerens navn, kontonummer eller det beløp eller betalingsdato som fremgår av betalingsoppdraget, er uriktig. Det kan også være at betaleren ombestemmer seg, fordi det oppdages at den vare eller tjeneste betaleren ønsket å gjøre opp for er beheftet med mangler og ønsker å utøve tilbakeholdsrett, kreve prisavslag, foreta motregning mv. Betaleren kan også ha ombestemt seg uten at det foreligger noen rimelig foranledning til det.

På den annen side tilsier målet om at betalingsoverføringer skal være effektive, at betalerens adgang til å tilbakekalle og endre ikke er for vid. I samme retning trekker hensynet til at en mottaker som er kjent med betalingsoppdraget, skal kunne stole på at oppdraget blir gjennomført. Med tanke på disse hensynene ble følgende bestemmelse inntatt i finansavtaleloven:

«**§ 28.** *Tilbakekall og endring*
(1) Tilbakekaller eller endrer betaleren et betalingsoppdrag, skal den institusjonen som forestår betalingsoverføringen, medvirke til dette. For en bestemt type betalingsoppdrag kan det likevel avtales at betaleren ikke skal kunne kreve tilbakekall eller endring.
(2) Et betalingsoppdrag kan ikke tilbakekalles eller endres etter at betaling har skjedd, jf. § 39 første ledd.
(3) For tilbakekall av sjekker gjelder reglene i sjekkloven.»

Første ledd første punktum pålegger institusjonen en plikt til å medvirke til at betalingsoppdrag tilbakekalles eller endres når betaleren krever dette. Institusjonens plikt gjelder uten hensyn til om tilbakekallingen eller endringen i forholdet mellom betaleren og mottakeren er rettmessig eller representerer mislighold. Ved konkurs vil konkursboet ha full adgang til å kreve institusjonens medvirkning til tilbakekall og endring av betalingsoppdrag som før åpningen av boet ble gitt

av konkursdebitor. Regelen i lovens § 28 betyr at institusjonen i utgangspunktet har plikt til å medvirke til tilbakekall og endring av betalingsoppdrag før betaling har skjedd. Betaleren har således krav på at institusjonen i rimelig utstrekning gjør det som er mulig for å tilbakekalle eller endre oppdraget. Medvirkningsplikten må blant annet vurderes ut fra hvor komplisert det er å tilbakekalle eller endre, den tid som er til rådighet, hvilke verdier som står på spill mv.

Med «tilbakekall» er det tenkt på de tilfeller hvor hele betalingsoppdraget trekkes tilbake. «Endring» vil foreligge når betalingsoppdraget i utgangspunktet opprettholdes, men betaleren for eksempel ber om endring av betalingsmottakerens navn, adresse eller kontonummer eller av beløpet eller tidspunktet for overføringen. Terminologisk vil et tilbakekall også være en endring, og det er derfor uten betydning å trekke en nærmere grense mellom tilbakekall og endring. Bestemmelsen gjelder også for betalingsoppdrag som ikke skal belastes innskuddskonto, jf. § 11 første ledd.

For enkelte typer betalingstjenester vil det kunne være behov for å avtale at betaleren ikke skal kunne kreve at institusjonene skal medvirke til tilbakekall eller endring. I annet punktum er det i samsvar med dette bestemt at «for en bestemt type betalingstjeneste kan det likevel avtales at betaleren ikke skal kunne kreve tilbakekall eller endring». Ordet «bestemt» er tatt inn for ikke generelt å åpne for klausuler i avtaler om betalingstjenester hvor betalerens rett etter første punktum er avskåret. Når praktiske hensyn sett i sammenheng med betalingstjenestens karakter tilsier at tilbakekall og endring ikke bør kunne kreves, kan slik avtale likevel inngås. Regelen er gjort ufravikelig i både forbruker- og næringsforhold, jf. lovens § 2 første og annet ledd. Departementet bemerket at det på dette området ikke var reelle grunner som skulle tilsi at det skulle være adgang til å avtale vilkår overfor næringsdrivende som stiller disse dårligere enn det som følger av loven, jf. Ot.prp. nr. 41 (1998-99) side 23. En avtale etter annet punktum vil isolert sett ikke hindre at institusjonen likevel medvirker til tilbakekall eller endring av et oppdrag om dette er mulig, men vil innebære at betaleren ikke kan kreve slik medvirkning.

Ved debetoverføringer vil det være tilfeller hvor institusjonen har forpliktet seg overfor mottakeren før betaling anses å ha skjedd. Når institusjonens forpliktelse er gitt i forståelse med betaleren, vil tilbakekall og endring være avskåret, jf. annet ledd. Her kan nevnes betalingskort hvor kortutstederen overfor mottaker har forpliktet seg til å honorere en anvisning og hvor kortholderen (betaleren) gjennom avtale har fraskrevet seg retten til å tilbakekalle og endre betalingsoverføringen. Ved bruk av betalingskort vil spørsmål om tilbakekall og endring normalt være regulert i avtalen mellom kortutstederen og kontohaveren, se ellers kapittel 4 nedenfor. Ved avtale om belastningsfullmakt vil det være lite aktuelt med tilbakekall eller endring av en enkelttransaksjon når overføringen er startet, fordi det vil være vanskelig å reversere transaksjonen, både på grunn av selve teknikken, og de forholdsvis korte tidsintervaller det her er snakk om, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 134. For tilbakekall av selve belastningsfullmakten vises til lovens § 26 siste ledd og avsnitt 2.3.2 foran. Når tilbakekallingen eller endringen av betalingsoverføringen har sin bakgrunn i forhold som betaleren svarer for, vil institusjonen kunne kreve å få dekket kostnadene som tilbakekallingen eller endringen har medført, etter alminnelige regler.

Etter annet ledd første punktum kan et betalingsoppdrag ikke tilbakekalles eller endres etter at betaling anses for å ha skjedd etter § 39 første ledd, se avsnitt 2.3.2 foran. Dette er yttergrensen for institusjonens plikt til å medvirke til tilbakekall og endring. Ved overføring til innskuddskonto vil dette si når mottakers institusjon er blitt forpliktet overfor mottakeren, noe som normalt skjer ved kreditering av mottakerens konto. Ved direkte overføringer med samtidig belastning og godskrivning av henholdsvis betalerens og mottakerens konto, vil tilbakekall være avskåret fra det tidspunkt betalingsordren effektueres. Ved kontant utbetaling av advisert giro, er skjæringstidspunktet for når tilbakekall og endring ikke lenger kan foretas, det tidspunkt beløpet stilles til mottakerens disposisjon på mottakerens sted, og melding om dette er kommet frem til mottakeren.

Hvis det er institusjonen som har begått en feil, for eksempel ved at den ved feilskrift har angitt galt kontonummer eller beløp, vil institusjonen være forpliktet til å rette feilen. For disse tilfeller gjelder ikke § 28, men reglene i §§ 32 og 33, se avsnitt 2.4 foran. Slik retting skal skje uavhengig av om beløpet er godskrevet mottakerens konto. Ved debetoverføring vil betaleren kunne tilbakekalle en betalingsoverføring ved å hindre at anvisningen blir betalt, for eksempel i form av tilbakekall av sjekk eller sperring av konto. Ved kreditoverføring som for eksempel papirbasert bankgiro, vil yttergrensene for betalerens rett til å tilbakekalle falle sammen med skjæringspunktene for når betaling har skjedd etter § 39 første ledd.

I bestemmelsens tredje ledd er det presisert at sjekklovens særregler om tilbakekall fortsatt skal gjelde for sjekker fremfor de alminnelige regler i § 28. Sjekker reguleres av lov av 27. mai 1932 nr. 3 om sjekker. Dette temaet drøftes ikke nærmere, ettersom utredningen her tar utgangspunkt i giro, betalingskort og andre nettbaserte betalingstjenester, se for øvrig avsnitt 1.1 foran.

2.6 Andres misbruk

2.6.1 Innledning

Finansavtalelovens kapittel 2 V inneholder flere bestemmelser som vedrører andres misbruk av bankkonto. Det er lovens § 34 som er hovedregelen om slikt misbruk. Bestemmelsen omfatter de tilfeller hvor kunden hevder at kontoen er blitt urettmessig belastet. Enkelte ganger vil det imidlertid kunne avdekkes at det er institusjonen selv som har begått en feil, typisk teknisk svikt eller lignende. I disse tilfeller gjelder ikke reglene i finansavtalelovens kapittel 2 V, men § 32 om feilaktig belastning av konto. Denne bestemmelsen er det redegjort for i avsnitt 2.5 foran.

Finansavtaleloven § 34 danner et utgangspunkt for misbruk av konto som er knyttet opp mot betalingsoverføringer. Alle former for betalingsoverføringer er videre knyttet opp mot tilgang og disponering av konto, enten det være seg betalingstjenester som giro, betalingskort eller annen nettbasert betalingsoverføring som nettbank og telefonbank. Tapssituasjoner oppstår slik sett i sammenheng med tilgang til en konto. Bestemmelsen i finansavtaleloven § 34 vedrører de tilfeller hvor belastningen er utført i samsvar med et betalingsoppdrag. Spørsmålet er da om belastningen har skjedd av en utenforstående, og om det er institusjonen eller kontohaveren som har risikoen for den urettmessige belastningen.

Det er ikke uvanlig at institusjonen gjør gjeldende at kontohaveren er å bebreide og har muliggjort andres misbruk, mens kontohaveren på sin side påstår at han eller hun ikke – eller i bare liten grad – er å laste. Ved elektronisk initierte betalingsoverføringer hvor PIN-kode brukes som identifikasjon, kan det videre være vanskelig å klarlegge om det er kontohaveren selv som har foretatt betalingsoverføringen eller om den er foretatt av andre. Ved slik brukerlegitimasjon ble det derfor foreslått særskilte regler, se avsnitt 2.6.3 nedenfor. De særskilte reglene vedrører misbruk av betalingskort og er regulert separat i § 35. *Banklovkommisjonen* fant at bruk av betalingskort reiser en del særegne spørsmål knyttet til ansvars- og risikovurderinger, og at en separat regulering var hensiktsmessig.

Finansavtaleloven § 34 angir de alminnelige regler for andres misbruk av konto, herunder tilknyttede betalingsinstrumenter. Reglene gjelder både for uttak i kontanter og belastninger. Uttak i kontanter kan skje i en banks betjente kasse eller i minibankautomat. Urettmessig belastning av konto kan for eksempel inntreffe ved girooverføring ved forfalsket underskrift eller legitimasjonsbevis. I merknadene til finansavtaleloven § 12 bokstav c) om betalingsinstrumenter, uttalte Banklovkommisjonen at eksempler på betalingsinstrumenter kan være sjekk, giroblanketter, betalingskort med eller uten kode, eventuelt i kombinasjon med terminaler som gir tilgang til betalings- eller kontokortsystemene. Videre fastslo Banklovkommisjonen, i sin utredning nr. 1 på side 110, at

> «[d]e tradisjonelle betalingsinstrumenter som er nevnt foran, kjennetegnes ved at de utstedes og kontrolleres av kontoførende institusjoner. Utviklingen går nå i retning av at en i økende grad også tar andre særskilte hjelpemidler i bruk, for eksempel telefon, bedriftsterminaler, eventuelt i kombinasjon med koder e.l. Betalingsinstrumenter representerer et vidt spekter av hjelpemidler som benyttes for å få adgang til betalingsmidler. Slik sett er det ingen prinsipiell forskjell mellom et tradisjonelt betalingsinstrument som giroblankett, og et moderne hjelpemiddel som telefon. Derimot vil ansvar og risikovurderinger kunne bli nokså ulike for instrumenter utstedt og kontrollert av institusjonen, og for hjelpemidler som betaleren selv eller en tredje part er eier av eller ansvarlig for (telefon, terminaler m.v.)».

For andre betalingstjenester enn betalingskort, er derved finansavtaleloven § 34 det rettslige utgangspunkt i forhold til potensielle tapssituasjoner som kan oppstå for kunden. Som sitatet viser, fastslo imidlertid Banklovkommisjonen at ansvars og risikovurderinger vil kunne bli nokså ulike med særlig vekt på hvilken del betaleren selv spiller ved den enkelte betalingsoverføring. Dette forholdet drøftes ikke nærmere i denne delen av utredningen, men er inntatt i avsnitt 6.1.2 under vurderingen av gjeldende ansvarsregulering for misbruk av nettbasert betalingsoverføring.

I tillegg til ansvarsregulering om andres misbruk av konto, er det gitt regler om lemping og tilbakeføring av beløp ved misbruk, som for øvrig også gjelder i forhold til misbruk av betalingskort. Disse reglene er inntatt i finansavtaleloven §§ 36 og

37 og gjennomgås i avsnittene 2.6.4 og 2.6.5 nedenfor.

2.6.2 Hovedregel – finansavtaleloven § 34

Hovedregelen om misbruk av konto mv. er gitt i finansavtaleloven § 34 og bestemmer følgende:

«**§ 34.** *Misbruk av konto m.v.*

(1) Kontohaveren er ikke ansvarlig for andres urettmessige uttak eller annen belastning med mindre den som har foretatt disposisjonen, har legitimert seg i samsvar med reglene i kontoavtalen, og belastningen har vært mulig som følge av forsett eller grov uaktsomhet fra kontohaveren eller fra noen som etter kontoavtalen har rett til å belaste kontoen.

(2) Ansvaret etter første ledd er begrenset til disponibelt beløp på kontoen på belastningstidspunktet. Er misbruk skjedd ved bruk av elektroniske betalingsinstrumenter innenlands, kan ansvaret heller ikke overskride belastningsgrenser som gjelder for den eller de bruksmåter som er benyttet. Begrensningene i leddet her gjelder ikke dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har medvirket forsettlig til at vedkommende kunne legitimere seg.

(3) Kontohaveren svarer ikke for andres urettmessige bruk som finner sted etter at institusjonen har fått varsel om forhold som skaper særlig fare for misbruk, som f.eks. at et betalingsinstrument er kommet bort eller at kode eller annen sikkerhetsprosedyre kan ha blitt tilgjengelig for uvedkommende. Kontohaveren er likevel ansvarlig dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, forsettlig har muliggjort bruken.

(4) Uten hensyn til reglene i denne paragrafen er kontohaveren i alle tilfelle ansvarlig for tap som skyldes at kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har utvist eller medvirket til svik mot institusjonen.

(5) Ansvaret ved misbruk av betalingskort er regulert i § 35.»

Som nevnt innledningsvis i avsnitt 2.1 foran, er store deler av den følgende beskrivelsen av bestemmelsen hentet fra Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag). Banklovkommisjonens forslag ble i stor grad fulgt opp av departementet i Ot.prp. nr. 41 (1998-1999) Om lov om finansavtaler og finansoppdrag.

Etter bestemmelsens første ledd stilles det to vilkår for at kontohaveren selv skal bli ansvarlig for andres uttak eller annen belastning av konto.

For det første må vedkommende som belastet kontoen, ha legitimert seg i samsvar med det som er bestemt i kontoavtalen, jf. finansavtaleloven § 16. Før en kontoavtale kan inngås, skal institusjonen opplyse om regler om hvordan kontoen og betalingsinstrument knyttet til kontoen kan brukes, herunder krav til legitimasjon, jf. lovens § 15 annet ledd bokstav d). Dersom den urettmessige belastning har skjedd uten at vedkommende legitimerer seg slik som fastsatt i kontoavtalen, vil kontohaveren – med det unntak som følger svikbestemmelsen i fjerde ledd – ikke kunne pålegges ansvar. Dette vilkåret følger som en naturlig konsekvens av institusjonens plikt til å påse at utbetaling skjer til rette vedkommende.

For det annet må belastningen ha vært mulig som følge av grov uaktsomhet eller forsett fra kontohaverens side. Lavere grad av uaktsomhet fører ikke til ansvar for kontohaver. Bestemmelsen i § 34 gjelder bare tilfeller hvor andre enn kontoinnehaveren har «legitimert seg i samsvar med reglene i kontoavtalen».

Annet ledd inneholder begrensninger i det ansvaret som følger av første ledd. Etter første punktum er kontohaverens ansvar i uaktsomhetstilfellene begrenset til disponibelt beløp på kontoen på belastningstidspunktet. I forarbeidene ble det antatt at de betalingstjenester som omfattes av bestemmelsen, er organisert slik at det i utgangspunktet ikke vil være mulig å trekke på en konto utover disponibelt beløp. Det ansvarstaket som disponibelt beløp representerer, faller dermed sammen med den øvre grensen for kontohaverens egen rett og mulighet til å trekke på konto.

Etter annet ledd annet punktum kan kontohaverens ansvar når elektroniske betalingsinstrumenter brukes innenlands, i uaktsomhetstilfellene heller ikke overstige periodebeløpet på transaksjonstidspunktet. Med «periodebeløp» menes her beløpsgrenser som for eksempel er fastsatt pr. uke for bruk av betalingsinstrumentet. Med begrepet «elektroniske betalingsinstrumenter» skal forstås instrumenter hvor dataene innsamles elektronisk.

Bestemmelsen i annet punktum vil blant annet gjelde for bedrifts- og hjemmeterminaler, jf. Banklovkommisjonens Utredning nr. 1 side 143 og drøftelsen foran avsnitt 2.6.1 om begrepet «betalingsinstrument». Derimot faller elektroniske overføringer som ikke er knyttet til bruk av elektroniske betalingsinstrumenter utenfor, for eksempel avtale om belastningsfullmakt, jf finansavtaleloven § 26. Banklovkommisjonen uttalte at elektroniske betalingskort på daværende tidspunkt var det mest typiske eksempel på elektroniske betalingsinstrumenter med innlagt periodebeløp.

I samsvar med dette må det legges til grunn at bankinstitusjonenes nettbanktjeneste kommer inn under denne regelen. I forhold til nettbanktjeneste er imidlertid ikke regelen like aktuell som en form for ansvarsbegrensning for kundens del, ettersom vedkommende som har fått tilgang til nettbankkontoen i stor grad kan styre dette selv, se avsnittene 6.1.2 og 6.2.3 nedenfor. Beløpsgrensene for nettbanktjenestene er dessuten forholdsvis høye sammenlignet med for eksempel betalingskortene.

Etter annet ledd tredje punktum gjelder ikke reglene i første og annet punktum dersom kontohaveren eller noen som har rett til å belaste kontoen, har medvirket forsettlig til at vedkommende har kunnet legitimere seg. Det ble lagt til grunn at kontohaveren i disse tilfellene ikke burde nyte godt av begrensningene i første og annet punktum.

Innføringen av tredje ledd var i hovedsak en kodifisering av gjeldende praksis. Bestemmelsen fritar kontohaveren for urettmessig bruk som finner sted etter at banken har fått varsel om at betalingsinstrument eller annen legitimasjon er kommet bort, med mindre kontohaveren eller noen som har rett til å belaste kontoen, forsettlig har muliggjort bruken.

Etter fjerde ledd er kontohaveren i alle tilfeller ansvarlig ved utvist svik mot institusjonen fra kontohaverens side eller fra noen som har rett til å belaste kontoen. Like med svik anses medvirkning til svik. I disse tilfellene gjelder således ingen av de begrensningene som følger av første til tredje ledd.

2.6.3 Særlige regler for betalingskort – finansavtaleloven § 35

For misbruk av betalingskort foreslo *Banklovkommisjonen* som nevnt foran avsnitt 2.6.2, i sin Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag), visse særskilte regler. Det ble ikke her gjort noe skille mellom debet- og kredittkortene. Reglene gjelder så langt det er benyttet personlig kode eller annen lignende sikkerhetsprosedyre i forbindelse med belastningen av betalingskortet, det vil si en form for brukerlegitimasjon som ikke er personavhengig som for eksempel signatur, stemmeprøve eller fingeravtrykk.

Banklovkommisjonen avga sin utredning 15. desember 1994. Bruken av elektroniske uttaks- og betalingskort hadde økt betydelig på daværende tidspunkt, og kortene var blitt en viktig del av hverdagen på linje med kontanter og datidens sjekker. I denne forbindelse ble forbrukernes rettstilling undersøkt nærmere. Det eksisterte ingen lovgivning som direkte regulerte forholdet mellom korthaver og kortholder, og *Banklovkommisjonen* uttalte, på side 67 i utredningen, at

> «det er av viktighet – både av hensyn til kortbrukerne og for å opprettholde tilliten til betalingskortsystemene – at sentrale ansvarsfordelingsspørsmål blir fastsatt i lov. Kommisjonen har derfor foreslått lovregler om ansvar for misbruk av betalingsinstrumenter».

Banklovkommisjonen foreslo en nærmere regulering av misbruk av betalingskort, som nå i det vesentligste er inntatt i finansavtaleloven § 35. Departementet uttalte, i Ot.prp. nr. 41 (1998-1999) side 43, at forslaget fremstår som en balansert helhetsløsning som tar i betraktning de ulike hensynene som gjør seg gjeldende på dette området. Bestemmelsen fastslår en ansvarsbegrensning for kunden ved andres urettmessige bruk av betalingskortet. Etter finansavtaleloven § 35 er følgende bestemt:

«**§ 35.** *Misbruk av betalingskort*

(1) Kontohaveren svarer med inntil kr 800 for tap som skyldes andres urettmessige bruk av betalingskort når tilhørende personlig kode eller annen lignende sikkerhetsprosedyre er brukt.

(2) Kontohaveren svarer med inntil kr 8.000 for tap som skyldes andres urettmessige bruk av betalingskort dersom

a) kontohaveren eller noen betalingskortet er overlatt til, ved grov uaktsomhet har muliggjort misbruket, eller
b) misbruket er muliggjort fordi kontohaveren eller noen betalingskortet er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at betalingskortet er kommet bort eller innen rimelig tid etter at dette burde vært oppdaget.

(3) Er misbruk av elektronisk betalingskort skjedd innenlands, kan ansvaret etter annet ledd ikke overskride de belastningsgrenser som gjelder for den eller de bruksmåter som er benyttet.

(4) Begrensningene i annet og tredje ledd gjelder ikke dersom kontohaveren eller noen kortet er overlatt til, forsettlig har muliggjort bruken av kortet. Begrensningene gjelder heller ikke for tap som er oppstått som følge av at kontohaveren eller noen kortet er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til irregulær bruk av kortet.

(5) § 34 tredje og fjerde ledd gjelder tilsvarende for kontohaverens ansvar etter paragrafen her.

(6) Kongen kan i forskrift bestemme at reglene i paragrafen her skal gjelde helt eller delvis for andre typer betalingsinstrumenter.»

I forhold til bestemmelsen i § 35 uttalte *Banklovkommisjonen* at kontohaveren etter første ledd skal ha et objektivt ansvar i form av en selvrisiko begrenset oppad til en egenandel som skyldes andres urettmessige bruk av betalingskort. Denne egenandelen ble etter departementets forslag satt til 800 kroner. Kontohaveren må, slik sett – uavhengig av egen skyld – dekke tap opp til egenandelen. Motstykket er imidlertid at kontohaveren, utover egenandelgrensen, overhodet ikke kommer i ansvar, med mindre kontohaveren eller noen betalingskort er overlatt til, ved grov uaktsomhet eller forsett har muliggjort misbruket. Det objektive ansvaret gjelder som nevnt bare for betalingskort som har tilknyttet personlig kode eller annen lignende sikkerhetsprosedyre. Det typiske ved slik identifikasjon er at dersom en utenforstående har kode og kort, vil vedkommende kunne benytte kortet uten å være berettiget til det. Det er hevdet at dette også omfatter såkalt «skimming» av kortet ettersom kortet her i prinsippet benyttes, men bare at det er en kopi av det. Det vises ellers til avsnitt 4.5 nedenfor.

Mens det objektive ansvaret etter første ledd er avgrenset til betalingskort med særlig sikkerhetsprosedyre, gjelder annet ledd for alle betalingskort, det vil si elektronisk eller manuelt benyttet uttaks-, debet- og kredittkort eller lignende kort for uttak eller overføring av betalingsmidler uten at det må inntastes en PIN-kode. Ansvarstaket innebærer en erkjennelse av at betalingskort i mange henseende er mer utsatt for misbruk enn andre betalingsinstrumenter.

Etter bokstav a) er ansvaret begrenset til 8.000 kroner dersom kontohaveren eller noen betalingskort er overlatt til, ved grov uaktsomhet har muliggjort misbruket. For at en handling eller unnlatelse skal kunne kvalifiseres som grov uaktsom, kreves det et markert avvik fra vanlig forsvarlig handlemåte. Avtaler om betalingskort vil som regel inneholde bestemmelser om bruk og oppbevaring av kort og eventuelle tilhørende koder. Det vil i så fall ligge et sett handlings- og adferdsregler til grunn for aktsomhetsvurderingen. Spørsmålet om når uforsiktig oppbevaring av betalingskortet er tilstrekkelig til å bringe korthaveren i ansvar etter annet ledd, må vurderes konkret. Dersom det i tillegg til kortet for eksempel stilles krav om bruk av en PIN-kode, må det foretas en samlet vurdering av oppbevaringen av både kort og kode.

Etter bokstav b) pålegges kontohaveren plikt til å foreta en viss kontroll og reagere snarest mulig når tap av betalingskort er oppdaget eller innen rimelig tid etter at tapet burde vært oppdaget. Her er ansvarsnormen vanlig uaktsomhet. Underretning til institusjonen er nødvendig både for å hindre ytterligere misbruk og for å sikre bevis.

Ansvarsbegrensningene gjelder ikke dersom kontohaveren forsettlig har muliggjort bruken. Ved forsett bærer kontohaveren som hovedregel hele risikoen for den urettmessige belastningen. Departementet var enig i dette unntaket og tilføyde at grensen heller ikke skulle gjelde der korthaveren får kjennskap til at kortet faktisk er misbrukt og likevel ikke underretter institusjonen. I en slik situasjon fremstår det som urimelig at korthaveren skal være beskyttet av beløpsgrensen.

2.6.4 Lempingsregel – finansavtaleloven § 36

Det er videre gitt regler om lemping av kontohaverens ansvar som gjelder både i forhold til finansavtaleloven §§ 34 og 35. Bestemmelsen er inntatt i lovens § 36 og fastslår følgende:

«**§ 36.** *Lemping av kontohaverens ansvar*

(1) Ansvaret etter §§ 34 og 35 kan lempes dersom måten kontoen kan disponeres på ikke er betryggende, eller dersom betalings- eller kontokortsystemet ikke oppfyller forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner, og den urettmessige belastning eller misbruket har sammenheng med dette. Det kan også tas hensyn til manglende aktsomhet eller andre forhold på institusjonens side som har medvirket til at den urettmessige belastningen eller misbruket kunne skje.

(2) Kontohaverens ansvar kan også nedsettes dersom en leverandør av varer eller tjenester som har mottatt betalingen, forsto eller burde forstå at bruken av betalingsinstrumentet var urettmessig.»

Selv om kontohaveren i utgangspunktet skulle være ansvarlig etter bestemmelsen om misbruk av betalingskort, er det fastslått at ansvaret kan reduseres helt eller delvis. Slik reduksjon kan skje dersom måten kontoen disponeres på ikke er betryggende og den urettmessige belastning har sammenheng med dette forhold. Kontohaverens ansvar kan reduseres eller falle bort helt eller delvis dersom betalings- eller kontokortsystemene ikke oppfyller forsvarlige standarder for identifikasjon-, kontroll- eller varslingsrutinger og den urettmessige belastningen har sammenheng med dette. Det kan for eksempel være tilfelle dersom

betalingskort kan brukes uten tilfredsstillende identitetskontroll eller andre forsvarlige sikkerhetsprosedyrer. Det samme er tilfelle om mangelfulle rutiner på institusjonens side har medvirket til at den urettmessige belastningen kunne skje.

Det er også bestemt, i annet punktum, at ansvaret kan nedsettes dersom manglende aktsomhet eller andre forhold på institusjonens side har medvirket til at den urettmessige belastningen eller misbruket kunne skje. Bestemmelsen vil for eksempel kunne ramme utbetaling av kontanter fra konto over skranke uten krav om fremleggelse av legitimasjon. Hvis legitimasjon fremlegges, men institusjonen må forstå at vedkommende som presenterer seg ikke er identisk med den som legitimasjonen gjelder, vil det også kunne være naturlig å lempe kontohaverens eventuelle ansvar.

Etter annet ledd kan ansvaret også reduseres eller falle bort dersom mottakeren forstod eller burde forstå, at bruken var urettmessig. Bestemmelsen legger opp til at institusjonene i avtaler med brukerstedene kan få inn klausuler om at mottakeren i disse tilfellene har ansvaret. I dag blir brukerstedene i liten grad stilt til ansvar for egen uaktsom opptreden. Bestemmelsen vil for eksempel kunne få betydning for butikk som mottar sjekker uten å kontrollere mot bankkort. Det samme gjelder manglende kontroll av betalingskort i manuelt system når det forutsettes kontroll av signatur eller bilde.

Bestemmelsen er en «kan»-regel, slik at vurderingen av om kontohaverens ansvar skal reduseres eller falle bort også vil bero på kontohaverens forhold. Dersom kontohaveren har opptrådt sterkt klanderverdig, vil det kunne være grunn til ikke å redusere kontohaverens ansvar selv om institusjonen er å bebreide.

2.6.5 Reklamasjon og tilbakeføring – finansavtaleloven § 37

Banklovkommisjonen var videre klar over et særlig problem ved urettmessige belastninger av konto: Ofte er beløpet allerede belastet kontoen på det tidspunktet tvisten om ansvarsforholdene mellom kontohaveren og institusjonen oppstår. Prosesskostnader forbundet med tvist om faktiske forhold kan ofte medføre at kontohaveren unnlater å anlegge sak for domstolene selv om denne mener at en belastning av konto er uhjemlet. Ettersom institusjonen på sin side har økonomisk evne til å forskuttere prosesskostnader og vil kunne pulverisere eventuelle tap ved misbruk på brukerkollektivet og betaling for tjenesten, foreslo *Banklovkommisjonen* å legge prosessbyrden på institusjonen. Banklovkommisjonens forslag ble i det vesentligste fulgt opp i finansavtaleloven § 37, og lyder som følger:

«**§ 37.** *Reklamasjon. Tilbakeføring*

(1) I den utstrekning kontohaveren ut fra reglene i § 34 eller § 35 bestrider å ha ansvar for en belastning, skal institusjonen tilbakeføre beløpet og erstatte rentetap fra belastningstidspunktet, forutsatt at kontohaveren setter frem krav om tilbakeføring uten ugrunnet opphold etter at denne ble eller burde ha blitt kjent med forholdet. Plikten til tilbakeføring etter første punktum gjelder ikke for egenandel etter § 35 første ledd.

(2) Første ledd gjelder ikke dersom

a) kontohaveren skriftlig har erkjent ansvar for belastningen, eller

b) institusjonen innen fire uker fra mottakelse av skriftlig innsigelse fra kontohaveren har anlagt søksmål eller brakt saken inn for en nemnd som nevnt i § 4 første ledd.

(3) Blir saken avvist av en nemnd eller en domstol, løper en ny frist på fire uker, fra den dagen institusjonen ble kjent med avvisningen.»

Etter første ledd må kontohaveren underrette institusjonen uten ugrunnet opphold etter at denne ble eller burde vært kjent med belastningen. Snarlig varsel er viktig både i relasjon til bevissikring og for å hindre ytterligere urettmessig bruk. Når institusjonen er blitt varslet, har denne på sin side plikt til å tilbakeføre beløpet og erstatte rentetap fra belastningstidspunktet. Institusjonen kan imidlertid gjøre fradrag for eventuell egenandel etter lovens § 35 første ledd som kontohaveren hefter for på objektivt grunnlag.

Spørsmålet om bevisbyrde oppstår særlig ved misbruk av betalingskort. Dette gjelder de tilfeller hvor korthaveren hevder at koden er oppbevart forsvarlig, men hvor koden likevel er benyttet ved uttaket. Bestemmelsen som ble foreslått og vedtatt, fastslår ikke en særskilt bevisbyrderegel på dette området. Begrunnelsen for dette er at det i praksis vil være kontohaveren som har best kjennskap til de faktiske forhold, blant annet om hvordan PIN-koden er oppbevart.

Plikten til tilbakeføring gjelder imidlertid ikke dersom kontohaveren erkjenner ansvar for belastningen, jf. annet ledd bokstav a). Et eksempel på dette vil være at betalingskort med tilhørende kode er gjort tilgjengelig for en person innen husstanden som har brukt kortet, og kontohaveren erkjenner ansvar for belastningen. Tilbakeførings-

plikten gjelder heller ikke dersom institusjonen innen fire uker etter at den har mottatt skriftlig innsigelse fra kontohaveren, anlegger søksmål eller bringer saken inn for nemnd, jf. bokstav b).

Etter tredje ledd har institusjonen en tilleggsfrist på fire uker dersom saken avvises fra klagenemndsbehandling. Dette gir institusjonen tid til å vurdere om den vil bringe saken inn for domstolsbehandling.

Når det gjelder aktuelle bevisspørsmål som ville kunne oppstå for en nemnd eller domstol, ble det fra departementets side, i Ot.prp. nr. 41 (1998-1999) side 44, understreket at

> «... selv uten en lovfestet bevisbyrderegel vil en nemnd eller en domstol ikke kunne legge til grunn at kunden har opptrådt grovt uaktsomt uten at det foreligger særskilte holdepunkter for dette. At PIN-koden er brukt uten at kunden har noen forklaring på hvordan koden er blitt kjent for uvedkommende, kan ikke være tilstrekkelig til å legge til grunn at kunden har opptrådt grovt uaktsomt og på dette grunnlag ilegge ansvar. Koden kan f.eks. ha blitt kjent for uvedkommende ved at misbrukeren, uten at kunden har merket det, har iakttatt kundens inntasting av kode i forbindelse med bruk av kortet.»

Bankklagenemndas praksis knyttet til urettmessig bruk av betalingskort viser at tilfelle hvor PIN-kode er brukt relativt kort tid etter at kortet ble stjålet og kortet ikke var i bruk like før dette, blir kunden som hovedregel holdt ansvarlig. I flertall av saker har det imidlertid vært dissens, og mindretallet har ikke funnet saken tilstrekkelig opplyst til at den bør realitetsbehandles. Det vises blant annet til Bankklagenemndas avgjørelser i BKN-02003, BKN-07131, BKN-08020, BKN-08026 og BKN-08027. Det vises for øvrig til avsnitt 6.3.2 punkt 2) nedenfor hvor lignende avgjørelser er kommentert nærmere.

Kapittel 3
Betalingsoverføring ved giro

3.1 Innledning

Ved bruk av giro gir betaleren sin bank instruks om å overføre et beløp til mottakeren fra egen konto. Banken vil undersøke om de nærmere bestemte betingelsene for å utføre oppdraget er oppfylt og deretter foreta overføringen. Disse betingelsene er noe avvikende alt etter hvilken giroform som velges av kunden. Det må i denne forbindelse skilles mellom girooverføringer som gjøres gjennom et kreditt- eller debetoverføringssystem.

I et kredittoverføringssystem går transaksjonen fra betaleren via formidleren til mottakeren. Det sies gjerne at denne form for betaling innebærer at man «skyver» betalingsmidlene gjennom systemet fra betaleren til mottakeren. Her finner man de vanligste formene for betalingsoverføring, som for eksempel bank- og brevgiro.

I et debetoverføringssystem er det motsatt. Her trekker mottakeren penger fra betaleren via formidleren. Betaleren må her gi mottakeren en tillatelse til å hente penger fra betalerens konto. Det tidligere brukte sjekksystemet er et eksempel på slike overføringsmekanismer. I dag er det særlig AvtaleGiro som brukes for direkte debitering for forbrukerbetalinger.

Betalingsoverføring ved bruk av giro kan på nåværende tidspunkt gjøres på flere måter. Det er her noen hovedskiller.

For det første kan kunden benytte seg av giroblanketter hvor han eller hun selv må utfylle betalingsinformasjonen. I denne gruppen finner man de tradisjonelle giroblankettene hvor kunden selv fyller ut informasjonen og tar den med til en bankfilial (bankgiro), benytter seg av brevgiroordningen eller foretar overføringen via sin nettbank. Slike girooverføringer via nettbank eller andre nettbaserte betalingstjenester er tema i kapittel 5 og utelates derfor i denne sammenheng. Girooverføringer enten direkte gjennom bank eller ved bruk av posten (brevgiro), er nærmere omtalt i avsnitt 3.2.1 nedenfor.

For det andre kan kunden benytte seg av ferdigutfylte giroblanketter, det vil si hvor kreditor har utfylt den nødvendige betalingsinformasjon og kunden bekrefter innbetalingen, enten gjennom signatur eller bekreftelse gjennom brukerlegitimasjon. I denne gruppen finnes giroordninger som papirbaserte ferdigutfylte giroblanketter og elektronisk giro. For de papirbaserte giroblankettene, kan kunden velge mellom å gå i banken, benytte seg av brevgiro eller foreta betalingen via sin nettbank. Elektronisk giro er som oftest direkte knyttet opp til en kundes nettbank, og er i stedet omtalt i avsnitt 5.2.1 nedenfor.

For det tredje er det mulig å foreta girooverføringer gjennom såkalt betalingsfullmakt. I denne gruppen finner man både AvtaleGiro og AutoGiro. Sistnevnte kan kun brukes i bedriftsmarkedet. I det følgende benyttes formuleringen «belastningsgiro» om disse betalingsformene. Belastningsgirering er tema i avsnitt 3.2.3 nedenfor. Slik giro er imidlertid i økende grad knyttet opp til kundens nettbankkonto. Hvordan belastningsgiro forholder seg til de nettbaserte betalingstjenestene, er omtalt i avsnitt 5.2.1 nedenfor.

I avsnitt 3.5 gis det en vurdering av reglene som gjelder for de aktuelle giroformene og det eventuelle lovgivningsbehovet.

3.2 Virkemåten

3.2.1 Bankgiro

Bankgiro er basert på bruk av papirblanketter hvor kunden fyller ut den nødvendige betalingsinformasjon og bekrefter oppdraget ved undertegning. Det må her skilles mellom de situasjoner hvor betaleren velger å oppsøke en bankfilial med en ferdig utfylt giroblankett eller velger å sende giroblanketter i forhåndsadresserte konvolutter. Sistnevnte form for betalingsoppdrag kalles for brevgiro. Girotjenestene har vært tilbudt i lang tid, henholdsvis siden 1946 og 1991. Det er kun grunnleggende betalingsfunksjoner som kan utføres ved bruk av slike giroblanketter, blant annet overføring fra konto til konto, kontant innbetaling til konto og fra konto til kontant utbetaling.

Hvorledes betalingsoverføringen gjennomføres, enten kunden benytter seg av girering direkte

i en bankfilial eller via posten, er forholdsvis sammenfallende. Dersom kunden skal benytte seg av overføring via *bankgiro,* leveres oppdraget direkte til en bank. Betaleren kan betale kontant eller velge å belaste sin bankkonto, så framt kunden har konto i den aktuelle banken. Kontant betaling innebærer som oftest et bankgebyr i tillegg til det påførte betalingsbeløpet. Slike gebyrer varierer fra bank til bank. Selve betalingsoppdraget initieres av at kunden signerer blanketten. Banken som tar imot bankgiroblanketten påtar seg oppdraget med å sende denne videre til Bankenes BetalingsSentral AS (BBS). BBS er den tjenesteleverandør som benyttes mest i forhold til betalingsoverføringer på nåværende tidspunkt, og som derfor benyttes som referansepunkt når betalingsoverføringsprosessen beskrives i den videre fremstillingen. Det nevnes at visse banker også har opprettet en tjeneste som heter «Bank i Butikk». Dette er en tjeneste som er knyttet opp til dagligvareforretninger hvor kunden – ved siden av å betale for varer i butikken – kan foreta uttak, innskudd, betale regninger eller heve giro for utbetaling. Det er således mange av de samme banktjenestene som kunden kan få utført i en bankfilial. Fordelen er imidlertid at butikkene som regel holder oppe lenger og flere dager i uken enn bankene.

Dersom kunden skal benytte seg av *brevgiro,* må kunden først inngå en avtale med sin bank og signere et kontrollkort. Signaturen leses elektronisk inn i BBS-systemet sammen med kundens navn, adresse og kontonummer. BBS sender deretter kunden et likt antall følgesedler og konvolutter. Ved bruk av brevgirotjenesten signerer kunden alle blankettene, noterer antall blanketter i konvolutten på følgeseddelen, signerer følgeseddelen og leverer konvolutten til sin bank eller sender den per post direkte til BBS. Deretter foretar BBS en elektronisk kontroll av signaturen på følgeseddelen mot den registrerte kontrollsignaturen, utfører eventuell dekningskontroll og registrerer giroblankettene på vanlig måte for avregning. Kunden mottar kvittering i form av en kvitteringsliste som viser de enkelte debiterte beløp og mottakers kontonummer.

3.2.2 Ferdigutfylte blanketter

Girooverføringer ved hjelp av ferdigutfylte blanketter, kan som nevnt innledningsvis utføres på forskjellige måter. Her omtales kun de papirbaserte giroer, mens elektronisk tilknyttede giroer er inntatt i avsnitt 5.2.1 nedenfor.

Ved *papirbasert giro* mottar kunden giroen i posten eller per e-post, såkalt e-postbasert giroblankett. Betaling av giroen kan for det første skje gjennom bank eller ved brevgiro hvor kunden påfører sin signatur og kontonummer. En annen mulighet er imidlertid at kunden foretar overføring via sin nettbank og er behandlet i avsnitt 5.2.1. Kunden må i begge tilfeller taste inn den informasjonen som kreditor har påført fakturaen.

3.2.3 Belastningsgiro

En tjeneste for automatisk betaling av faste regninger ble lansert i 1995. Fra 2000 ble det foretatt et skille mellom privatpersoner og bedriftskunder, slik at AvtaleGiro kun benyttes av privatpersoner og AutoGiro av bedriftskunder. De overordnede prinsippene er imidlertid de samme. Dette er en ordning med direkte debitering som gir kreditor mulighet til å belaste kundens konto ved forfall. Slik belastningsgirosystemet er bygd opp, inngår kunden og kreditor generelle avtaler med sine institusjoner om at betalinger kan skje gjennom denne ordningen. Den konkrete debiteringsordningen mellom partene kommer i stand ved at betaleren, på eget initiativ eller på oppfordring fra mottakeren, gir sin institusjon fullmakt til å etterkomme debiteringskrav fra mottakeren. Dette vil for så vidt bestå i faste beløpsgrenser og gir uttrykk for definerte gjeldsforhold. Institusjonen sender så melding om dette til mottakeren og hans institusjon.

Ved belastningsgiro betales regningene direkte fra kundens konto på forfallsdato uten at kunden må gjøre noe aktivt. Beløpet blir således trukket fra kundens konto til de avtalte periodene uten at kunden nødvendigvis aksepterer dette, sml. motsetningsvis ordningen med eFaktura i avsnitt 5.2.1 nedenfor. Kunden blir imidlertid varslet om trekket (for eksempel ved brev, e-post eller SMS) og beløpets størrelse før betalingen gjennomføres, og har mulighet til å stoppe en betaling. Kunden har slik sett tilnærmet lik kontroll som ved manuell betaling. På den annen side er det hevdet at kunden lettere kan miste oversikten over belastningene på kontoen, se Ot.prp. nr. 41 (1998-1999) side 30. Forskjellen fra eFaktura, er at belastningsgiroer belaster kontoen dersom kunden ikke stopper belastningen i tide.

3.3 Feil fra kundens side

3.3.1 Risiko

Et viktig risikoforhold som gjelder tap i forbindelse med betalingsoverføringer ved hjelp av giro, er feil

fra kunden selv. *Banklovkommisjonen* har vurdert dette opp mot de forskjellige gireringsformene som er beskrevet i avsnittene foran.

1) De tenkelige tapssituasjoner som kan oppstå som følge av forhold på kundens side ved bruk av *bankgiro,* er av begrenset omfang. Det er særlig feilskrift som er aktuelt i denne sammenhengen. Dette kan blant annet bero på at kunden påfører feil beløp eller feil kontonummer, men likevel sender oppdraget til behandling. Slike feil kan tenkes å bli oppdaget, enten av kunden selv eller av institusjonen som mottar oppdraget. *Banklovkommisjonen* har særlig undersøkt sikkerhetsrutinene i forhold til institusjonene og deres videre behandling av betalingsoppdraget. Det kan for eksempel tenkes at det eksisterer et system hvor det foretas en kryssjekk mellom påført kontonummer og mottakers navn og adresse. Ifølge BBS eksisterer det imidlertid ikke et slikt system. I flere av bankenes kontoavtaler er dette også eksplisitt kommet til uttrykk, eksempelvis formulert som at beløpet vil bli overført til oppgitt kontonummer, selv om oppgitt kontonummer tilhører en annen enn den mottaker som er oppgitt med navn og adresse på giroblanketten. I de fleste tilfeller hvor det påføres feil kontonummer, er imidlertid dette et ugyldig kontonummer, slik at belastningen ikke utføres. Det er langt vanligere at beløpsfeil fører til utilsiktede belastninger av kundens konto. BBS har opplyst at påføring av feil beløp totalt sett i gjennomsnitt skjer én gang per dag, det vil si ca. 350 enkelttilfeller i året.

Risikoen for at det oppstår tapssituasjoner som følge av kundens egne feil ved bruk av bankgiro, har imidlertid *Banklovkommisjonen* vurdert som forholdsvis liten. Selve det papirbaserte formatet og forutsetningen om at kunden selv må håndskrive den nødvendige betalingsinformasjon, gir kunden en større anledning til å undersøke at det er påført riktig betalingsinformasjon enn ved for eksempel nettbank. Slik girering forutsetter heller ikke at kunden må forholde seg til andre forhold av systemteknisk art. Det kreves for det første ikke at kunden legitimerer seg med personlige opplysninger som ved nettbaserte betalingsoverføringer for å kunne påskrive betalingsinformasjonen. For det andre kreves det ikke at kunden påfører noen form for engangskode eller lignende for at betalingsoppdraget kan behandles. Totalt sett fremstår denne girotjenesten derfor ikke som et betalingsoverføringssystem som er eksponert for de helt store risikoaspekter.

Bruk av de tradisjonelle giroblankettene er dessuten nedadgående. Allerede i 2002 ble flere giroer betalt via nettbank enn via brevgiro og for så vidt også telegiro.[1] Privatkunder foretok 154 millioner nettbankbetalinger mot 29 millioner betalinger via brevgiro i 2007. Etter det Banklovkommisjonen har fått opplyst fra BBS, har det heller ikke oppstått tapssituasjoner av større betydning for kundene. Det henger blant annet sammen med rutinene for korrigeringer av betalingsoppdrag, enten det gjelder korrigering av beløpsfeil og/eller kredittkonto: I løpet av kort tid (innen 3 dager) etter at BBS er blitt opplyst om at det har forekommet en feil, sendes det brev til banken med informasjon om korrigeringen hvor det samtidig bes om at banken informerer kunden. Deretter sendes det brev til kunden som har fått godskrevet pengene hvor det bes om fullmakt til å trekke ut pengene. Den dagen korrigeringen skal finne sted, kontakter BBS den aktuelle banken for å få utført en dekningskontroll.

Banklovkommisjonen finner grunn til å nevne at feil også kan forekomme i den forstand at kunden betaler en regning to ganger. Det er sett eksempler på at Posten har sendt ut allerede betalte regninger. Slike tilfeller vil imidlertid bli rettet opp av Posten så snart det blir oppdaget, og kan ikke sies å representere et stort faremoment i denne sammenheng.

2) Aktuelle risikoforhold ved bruk av ferdigutfylte blanketter er av begrenset omfang. Når det gjelder de papirbaserte ferdigutfylte giroblankettene, vil det – ved bruk av bank- og brevgiroblanketter – vanskelig tenkes å forekomme feil som er forårsaket av kunden selv. I disse tilfellene kreves det kun en underskrift fra kundens side i tillegg til angivelse av det kontonummer som skal belastes. Dersom det er oppført galt kreditkontonummer, er dette et forhold som kreditor må ta følgene av. Kunden kan ikke i slike tilfeller pålegges ansvar.

3) De risikoelementer som eksisterer ved bruk av belastningsgiro, må anses å være av ubetydelig karakter. Når det gjelder avtaleinngåelsen om en slik ordning, vises det til finansavtalelovens regler. Det kan vanskelig tenkes at det oppstår tap som følge av kundens egne feil: Kundens delaktighet i de enkelte betalinger er mer eller mindre lik null. Så lenge de generelle avtalene er inngått, er kundens eneste valg å stoppe en belastning. Det kreves med andre ord ingen aktiv opptreden fra kundens side. De feiloverføringer som måtte forekomme, må på samme vis som ved de ferdigutfylte blankettene, være forhold som kreditor står ansvarlig for.

[1] Norges Banks årsrapport om betalingssystem 2007.

3.3.2 Ansvarsregulering

Tap som følge av kundens egne feil ved bruk av giro, vil i første rekke være aktuelt ved betalingsoverføring via bankgiro. I disse tilfellene er det kunden selv som må fylle inn betalingsinformasjonen, og det er i denne prosessen mulig at kunden gjør feil som fører til en utilsiktet betalingsoverføring. For ferdigutfylte giroblanketter er det lite rom for feil fra kundens side. Her er betalingsinformasjonen allerede utfylt, slik at eventuelle feiloverføringer må anses som et forhold som kreditor må bære risikoen for. Den følgende beskrivelse av aktuell ansvarsregulering i situasjoner hvor kunden har gjort en feil, gjelder således først og fremst i forhold til bankgiro. For belastningsgiro er det gitt egne regler. Disse omtales til slutt i dette avsnittet.

1) Dersom det skulle oppstå tap som følge av kundens feilbruk av bankgiro, er utgangspunktet at kunden står fullt ut ansvarlig. Dette følger først og fremst av bankenes kontoavtaler som nevnt i avsnitt 3.3.1 foran. Dette er også slått fast i praksis, og *Banklovkommisjonen* viser i den anledning eksempelvis til Bankklagenemndas sak BKN-01075. Her la nemnda til grunn at kunden feilaktig hadde gitt banken i oppdrag å overføre to beløp til samme kontonummer, og at kunden derved måtte stå ansvarlig for den omstridte disposisjonen.

Spørsmålet er imidlertid om kunden, etter gjeldende lovbestemmelser, har anledning til å tilbakekalle beløpet dersom vedkommende i ettertid har oppdaget at det enten er påført feil mottaker eller beløp. Denne muligheten er begrenset og er knyttet opp til det tidspunkt en finansinstitusjonen mottar betalingsoppdraget, jf. finansavtaleloven § 28 annet ledd, jf. lovens § 39 annet ledd bokstav a), se avsnitt 2.3.2 og 2.5 foran. I denne sammenheng må det skilles mellom girobelastning i bank og girobelastning ved bruk av brevgirotjenesten.

I førstnevnte tilfelle vil kundens adgang til å tilbakekalle være avskåret fra bankfunksjonæren har mottatt giroen og verifisert denne ved stempel eller lignende. I forhold til brevgiro, er prosessen annerledes idet kunden sender giroblanketten per post til BBS. Det tradisjonelle utgangspunktet er her at kunden kan tilbakekalle betalingsoppdragene, så lenge kunden har kontaktet BBS om dette før BBS har mottatt følgesedlene, sml. avtaleloven § 7. Dette følger også av standardvilkårene i kontoavtalen. Ifølge BBS er imidlertid rutinene i praksis noe annerledes: Dersom kunden oppdager at det er gjort en feil, kan vedkommende ringe inn til BBS' kundeservice. Her må kunden identifisere seg gjennom noen kontroll- og verifikasjonsspørsmål. Deretter kan kunden forklare hvilke giroblanketter det gjelder. BBS legger deretter inn en sperre på følgeseddelen, men garanterer ikke at det aktuelle betalingsoppdraget likevel vil kunne bli gjennomført. Det kommer an på hvor langt oppdragene er kommet i BBS' systemer. Slik sett er ikke kunden sikret tilbakekall av utilsiktede betalingsoppdrag etter at vedkommende har postlagt giroblankettene. Det kan stilles spørsmålstegn ved om dette tilfredsstiller de lovmessige kravene til frist for tilbakekalling, jf. avtaleloven §§ 28 og 39. Systemtekniske forhold i avregningen mellom bankene gjør det imidlertid nødvendig å begrense sluttidspunktet for tilbakekall av betalingsoppdrag, jf. også krav fra Norges Bank som konsesjonsmyndighet etter betalingssystemloven om fastsettelse av tidspunkt for når oppdrag skal anses mottatt i avregningen. Det skal her tilføyes at finansavtaleloven § 28 første ledd åpner for avtale om at tilbakekall ikke skal kunne finne sted for bestemte typer betalingsoppdrag. Rutinene rundt avregningssystemene og tilbakekallsmuligheten i forbindelse med nettbanktransaksjoner drøftes i avsnitt 6.2.4 nedenfor.

En annen mulighet er for så vidt at betaleren melder fra til den utilsiktede mottakeren av pengene, jf. for så vidt avtaleloven § 7. Dette er imidlertid ikke en forutsetning for at mottakeren skal fratas retten til de overførte pengene. I henhold til blant annet avtaleloven §§ 32 og 33 vil mottakeren ikke ha krav på pengene så langt denne innså eller burde innsett at det var penger som ikke rettmessig kan disponeres av vedkommende. Bestemmelsene må imidlertid sees i sammenheng med kontoavtalene til bankene, hvor det er fastsatt at oppdrag på basis av giroblanketter vil utføres selv om kontonummer og mottagers navn ikke er korresponderende. Betydningen av bestemmelsen i avtaleloven må således sies å ha begrenset betydning i forhold til bankgiro. Reglene vil uansett ikke kunne avhjelpe den potensielle tapssituasjonen dersom mottakeren likevel bruker pengene og deretter går personlig konkurs, sml. saken med uriktig overføring av 500.000 kroner gjennom nettbank som er kommentert nærmere i avsnitt 5.4.1 nedenfor.

Videre er det ikke inntatt noen bestemmelser om slike utilsiktede betalingsoverføringer i finansavtaleloven. Det er for så vidt inntatt regler om henholdsvis feilaktig godskriving og belastning av en kundes konto, jf. finansavtaleloven §§ 31 og 32, se avsnitt 2.4 foran. Disse reglene vedrører imidlertid feil fra institusjonens side. I Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 141-142, ble det fastslått at bestemmelsene ikke gjelder dersom det er andre

enn banken selv eller dennes medhjelpere som har initiert transaksjonen. I slike tilfeller ble det forutsatt at finansavtalelovens bestemmelser i kapittel 2 V skal gjelde. Her er det imidlertid kun gitt bestemmelser om andres misbruk, jf. finansavtaleloven § 34 flg. For andre betalingsinstrumenter enn betalingskort, er det heller ikke inntatt særlige lovbestemmelser som eventuelt skulle gi kunden et begrenset ansvar, sml. betalingskortreglene i lovens § 35.

2) Selv om risikoen for at kunden gjør feil ved bruk av belastningsgiro er av ubetydelig karakter, er det likevel inntatt regler om slike belastningsfullmakter i finansavtaleloven § 26. Dette vedrører både avtaleinngåelsen og de enkelte belastningene. Begrunnelsen for dette var likevel ikke knyttet til tap som følge av kundens egne feil eller tredjemanns misbruk. *Banklovkommisjonen* anså på generelt grunnlag flere faremomenter tilknyttet slike belastninger, det ble derfor foreslått visse regler for at slike belastninger skulle skje i mer betryggende former. Det vises for øvrig til avsnitt 2.3.3 foran.

3.3.3 Vurdering

Etter *Banklovkommisjonens* oppfatning er risikoen for at det oppstår tap som følge av feilbruk av *ferdigutfylte giroblanketter* og *belastningsgiro,* av forholdsvis begrenset karakter. Dette forholdet gjør seg dess mer gjeldende når risikoelementene sees i sammenheng med den gjeldende ansvarsregulering. Som redegjørelsen i avsnittet foran viser, kan det vanskelig tenkes at kunden vil bli holdt ansvarlig dersom det oppstår tap som følge av feilaktige betalingsoverføringer. De eksisterende reglene på området, anser derfor *Banklovkommisjonen* som tilfredsstillende og nødvendiggjør ikke en ytterligere regulering av slike betalingstjenester.

Når det gjelder bankgiro basert på kundeutfylte blanketter, er det imidlertid flere risikoforhold som gjør seg gjeldende og potensiell feilbruk med påfølgende tap er derfor mer fremtredende. Det rettslige utgangspunktet for tap som oppstår som følge av kundens egne feil, er dessuten at kunden holdes ansvarlig. Dette innebærer at feilskrift og utilsiktede betalingsoverføringer som hovedregel ikke kan kreves rettet eller dekket av institusjonen. Slik sett vil kunden stå fullt ansvarlig for de tap som måtte oppstå som følge av feilskrift på giroblankettene. Spørsmålet er om dette er en rimelig løsning, eller om det, i tråd med forutsetningene i mandatet, bør foreslås en rettslig regulering som kan lempe på slike potensielle tapssituasjoner. Dette redegjøres det for nærmere i avsnitt 3.5 nedenfor.

3.4 Andres misbruk

3.4.1 Risiko

I tillegg til risikoen for at kunden utfører en utilsiktet betalingsoverføring ved bruk av de ulike girotjenestene beskrevet i avsnitt 3.2 foran, har *Banklovkommisjonen* funnet grunn til å omtale risikoen for at tredjemann misbruker disse tjenestene. Som ved risikobeskrivelsen i forhold til kundens egne feil, er det også her skilt mellom bankgiro, ferdigutfylte giroblanketter og belastningsgiro.

1) De aktuelle misbrukstilfellene i forhold til bruk av bankgiro vil typisk bestå i at signaturen er falsk. Risikoen for at slik forfalskning medfører et tap for kunden forutsetter at bankens systemer ikke fanger opp dette ved hjelp av sine sikkerhetsrutiner. Her må det skilles mellom sikkerhetsrutiner knyttet til tradisjonell bruk av bankgiro, hvor kunden oppsøker en bankfilial, og sikkerhetsforordninger knyttet til bruk av brevgirotjenesten, hvor kunden sender bankgiroen(e) per post direkte til BBS for belastning.

Ved *bruk av bankgiro* vil misbruket kunne oppstå ved at en person oppgir falsk legitimasjon og påtegner falsk underskrift uten at bankfunksjonæren oppdager dette og iverksetter urettmessig uttak eller belastning. *Banklovkommisjonen* antar at potensielle tapssituasjoner for slikt misbruk likevel er noe begrenset. Det kreves et forholdsvis vel gjennomført svindelopplegg hvor tredjemann enten forsøker å utgi seg for å være kunden eller har tilegnet seg tilstrekkelige opplysninger til å produsere et falskt legitimasjonsbevis. Risikoen for slike svindelopplegg må videre sees i sammenheng med bankenes rutiner ved girobelastning i skrankene. Banklovkommisjonen har mottatt informasjon fra en rekke banker angående de sikkerhets- og legitimasjonsrutiner som følges ved slike betalingsoverføringer. Dersom vedkommende i skranken kjenner vedkommende som innleverer oppdraget, er som oftest rutinen at det ikke kreves legitimasjonsbevis. En faktor som beløpets størrelse vil imidlertid kunne spille inn, også i forhold til kjente kunder. Hvis kunden ikke er kjent, kreves det vanligvis legitimasjon. Praksis fra bankene viser imidlertid at dette ikke alltid er tilfelle. *Banklovkommisjonen* er også usikker på sikkerhetsrutinene tilknyttet banktjenesten «Bank i Butikk» som er kort beskrevet i avsnitt 3.2.1 foran. Dette er en forholdsvis ny tjeneste og det er på

nåværende tidspunkt vanskelig å si noe om rutiner og praksis i forbindelse med innlevering av betalingsoppdrag til dagligvareforretninger mv.

Krav om legitimasjonskontroll vil uansett ikke alltid være til hjelp dersom det dreier seg om falske legitimasjonspapirer som den bankansatte ikke oppdager. Det finnes flere eksempler på identitetstyverier som medfører produksjon av falske legitimasjonsdokumenter, men *Banklovkommisjonen* antar at slike svindeltiltak har minsket i takt med den økte bruken av betalingskort og nettbasert betalingsoverføring hvor tilgang kun er betinget av brukerlegitimasjon ved hjelp av kode og annet sikkerhetsverktøy.

Ved *bruk av brevgirotjenesten* kan det være tilstrekkelig at tredjemann får tak i kundens følgesedler og påfører falsk underskrift. Dersom ikke systemene fanger opp dette ved sin signatur- og kontokontroll (det vil si at signaturen og kontonummeret korresponderer), vil betalingen kunne gjennomføres.

Ifølge BBS er det flere typetilfeller av slikt misbruk. Det er særlig misbruk fra et av medlemmene i kundens husstand eller familie som utpeker seg.[2] Selv om gjerningspersonen er kjent for kunden, er det imidlertid flere forhold som medfører at kunden som oftest ikke får tilbakeført pengene. For det første krever BBS at slik forfalskning politianmeldes av kunden, jf. også avsnitt 3.4.2 nedenfor. I de fleste tilfeller ønsker imidlertid ikke kunden å forfølge saken, ettersom det dreier seg om nærstående personer, og tar tapet selv. For det andre vil det i slike saker være flere kompliserte faktaforhold knyttet til for eksempel fullmaktsforhold, som gjør at saken i første omgang blir avvist av Bankklagenemnda. Så framt det ikke dreier seg om de helt store beløpene, er det uvanlig at kunden velger å ta saken videre til domstolene. Her vil omkostningene ofte kunne bli store, og en forfølgelse av saken vil slik sett kunne koste mer enn hva de(n) urettmessige belastningen(e) har beløpt seg til. Statistikk fra domstolene viser også at slike saker sjelden blir fremmet.

Forfalskning av selve følgesedlene kan også forekomme, men BBS er forsikret mot slik svindel og risikoen for at kunden påføres et tap i slike situasjoner er derfor liten.

Misbruk kan også forekomme ved at tredjemann bryter seg inn i kundens bolig og tilegner seg brevgiroblankettene for deretter å påføre falsk underskrift. BBS har også informert om at innbrudd i Postens egne postkasser, enten ved å bryte opp postkassen eller «lirke» ut brev med følgeseddel og giroblanketter, er et ikke uvanlig fenomen som har medført at det er foretatt urettmessige belastninger ved hjelp av brevgiroblanketter. Ettersom det normalt kun stilles krav om at kunden noterer ned antallet giroblanketter på følgeseddelen som skal belastes og signerer, er det her mulig å bytte ut kundens giroblankett med en annen. Av hensyn til brukervennlighet av tjenesten er det ikke stilt krav om at det på følgeseddelen noteres hvilke fakturaer det gjelder, noe som kunne forhindret slikt misbruk.

2) Tredjemanns misbruk knyttet til bruk av ferdigutfylte giroblanketter, må anses å utgjøre en begrenset risikofaktor for at det oppstår tap på kundens hånd. Det er etter *Banklovkommisjonen* oppfatning likevel hensiktsmessig å gi en kort fremstilling av risikoforhold og ansvarsregulering som knytter seg til dette temaet.

Ferdigutfylte giroblanketter utstedes som oftest av etablerte foretak eller institusjoner. Sannsynligheten for at tredjemenn klarer å produsere slike fakturaer og at kunden iverksetter en betaling – til et fiktivt selskap – må anses som svært liten. Slike giroblanketter vil jo være knyttet opp mot et gjeldsforhold mellom kunden og kreditor, som kunden til dels må antas å ha grei oversikt over. Fakturaen vil i alle tilfelle være uberettiget. Det kan likevel tenkes tilfeller hvor tredjemann urettmessig får tilgang til et foretaks regnskapssystem og endrer betalingsinformasjonen. I slike situasjoner er det uansett klart at kunden ikke kan holdes ansvarlig, og at dette er et misbruksforhold som påhviler kreditor.

Tredjemenn kan imidlertid utferdige falske ferdigutfylte giroblanketter som for eksempel angivelig skal gå til «en god sak» eller er del av en fiktiv innsamlingsaksjon. Slikt svindelforsøk har skjedd i praksis, men blir som oftest raskt oppdaget og formidlet videre til kundene. Tapspotensialet må derfor også her anses som begrenset.

3) Ettersom belastningsgiro er betinget at av kunden inngår en avtale med kreditor med de respektive institusjoner som mellomledd, jf. avsnitt 3.2.3 foran, kan det vanskelig tenkes å oppstå misbrukstilfeller. Det er flere forhold som må være klarlagt før avtale om belastningsfullmakt er gyldig, og det må antas at kunden i denne prosessen blir skjermet mot eventuelle misbruksforsøk fra tredjemenn, for eksempel ved at det er en fiktiv kreditor.

[2] Det forutsettes i denne sammenheng at det ikke dreier seg om personer som etter kundens kontoavtale har rett til å belaste kontoen, jf. finansavtaleloven § 34 første ledd in fine.

3.4.2 Ansvarsregulering

1) Tap som følge av andres misbruk knyttet til bruk av bankgiro, kan som redegjørelsen i avsnittet foran viser, oppstå i flere tilfeller. Hovedregelen etter finansavtaleloven § 34 er at kunden ikke står ansvarlig for andres misbruk av sin konto. Dette må også sees i sammenheng med avtalerettslige regler, se særlig avtaleloven §§ 33 og 36. Falsk underskrift vil eksempelvis klart falle under avtalerettslige prinsipper om ugyldige viljeserklæringer. Kunden vil imidlertid kunne bli erstatningsansvarlig dersom han eller hun ved uaktsom opptreden har medvirket til misbruket. Det stilles etter finansavtaleloven krav om grov uaktsomhet eller forsett. Lavere grad av uaktsomhet fører således ikke til ansvar for kunden. Det vises til avsnitt 2.6.2 foran. Det nevnes ellers at institusjonen har ansvar for å rette opp feilbelastninger som er utført av institusjonen selv, jf. finansavtaleloven § 32 og avsnitt 2.4 foran.

Det skilles også her mellom bankgiro belastet direkte i bankfilial og bankgiro som sendes per post til BBS (brevgiro). For bankgiro som innleveres og belastes i bankfilial, er det som redegjørelsen foran avsnitt 3.4.1 viser, rimelig å anta at misbrukstilfellene er av begrenset omfang. Dersom tredjemann klarer å tilegne seg kundens legitimasjonskort og/eller opplysninger som gjør at et falskt legitimasjonsbevis kan produseres, er regelen uansett klar: Kunden er ikke erstatningsansvarlig, jf. finansavtaleloven § 34. Det kan videre vanskelig tenkes at kunden i slike tilfeller skal anses å ha opptrådt grovt uaktsomt. Det vil som oftest dreie seg om innbrudd i kundens bolig eller postkasse som ikke kunden kan lastes for. Det må imidlertid tas forbehold for de tilfeller hvor kunden ikke setter frem krav om tilbakeføring uten ugrunnet opphold etter at kunden ble, eller burde ha blitt, kjent med forholdet, jf. finansavtaleloven § 37 første ledd første punktum, se også avsnitt 2.6.5 foran.

For bankgiro som innleveres gjennom brevgirotjenesten, vil det samme gjelde dersom det dreier seg om innbrudd i bolig eller postkasse og urettmessig bruk av stjålne brevgiroblanketter. BBS har tegnet forsikring mot slikt misbruk og kunden holdes i disse tilfeller derfor skadesløs, så framt saken politianmeldes av kunden selv. Hvor det dreier seg om urettmessig belastning som er forårsaket av noen i kundens husstand eller lignende, er utgangspunktet også det samme. Som vist i avsnitt 3.4.1 foran, er imidlertid tapsrisikoen her større, ettersom de fleste kvier seg for å politianmelde noen som er nærstående. Det kan videre oppstå tilfeller hvor faktum er uklart med henhold til for eksempel avgitte fullmakter som kunden hevder ikke å stå inne for.

2) Som vist foran avsnitt 3.4.1 har *Banklovkommisjonen* ansett potensielle tapsforhold ved misbruk i forbindelse med bruk av ferdigutfylt giroblankett og belastningsfullmakt som forholdsvis begrenset. Dette er særlig begrunnet i selve prosesseringsmåten av slike giroer og at tredjemann må få tilgang til systemer som er sikret i større og mer profesjonell grad enn systemet for belastning av vanlig bankgiroer. *Banklovkommisjonen* har derfor ikke funnet grunn til å gå nærmere inn på ansvarsspørsmålet for disse formene for girobelastninger, ettersom kunden som oftest ikke vil lide et økonomisk tap.

3.4.3 Vurdering

Etter gjeldende lovgivning er kunden bare erstatningsansvarlig for oppståtte tap som følge av misbruk av betalingstjenesten dersom gjerningspersonen har legitimert seg i samsvar med kontoavtalen og kunden har muliggjort dette ved grov uaktsom eller forsettlig handlemåte, jf. finansavtaleloven § 34 første ledd, se også avsnitt 2.6.2. Visse begrensninger følger også av annet og tredje ledd. Spørsmålet er imidlertid om denne reguleringen er tilfredsstillende eller om det bør vurderes å innføre nærmere regler som for eksempel en tapsbegrensning ved oppstått tap på kundens hånd, jf. betalingskortreglene i finansavtaleloven § 35. Dette er drøftet i avsnitt 3.5 nedenfor.

3.5 Lovgivningsbehovet

Foran er det redegjort for betalingsoverføringer ved hjelp av ulike girotjenester. Dette omfatter bankgiro, ferdigutfylte giroblanketter og belastningsgiro som AutoGiro og AvtaleGiro. For hver av giroformene er det for det første gitt en beskrivelse av tjenestenes virkemåte. For det andre er det redegjort for aktuelle risikoforhold som er tilknyttet betalingsoverføring ved bruk av slike giroformer. For det tredje er det gitt en oversikt over gjeldende ansvarsregulering ved oppståtte tapssituasjoner, enten som følge av feilbruk eller misbruk. Som *Banklovkommisjonens* gjennomgang og vurdering av ferdigutfylte blanketter og AvtaleGiro viser, kan det ikke sies å være et særlig behov for noen nærmere regulering av disse gireringsformene. Det vises her til avsnitt 3.3.3 og 3.4.2 punkt 2) foran. I det følgende tas det dermed utgangspunkt i giro som leveres direkte i bank (bankgiro)

og giro som sendes per post (brevgiro) hvor kunden selv må påføre den nødvendige betalingsinformasjon.

3.5.1 Kundens egne feil

1) Når det gjelder økonomisk tap som har oppstått ved bruk av bankgiro som følge av kundens egne feil, er det flere momenter som tilsier at det er kunden som bør stå ansvarlig. Det er først og fremst feilskrift som kan forårsake feiloverføringer i slike tilfeller. I den forbindelse er det visse forhold som må vektlegges og som for så vidt også gjelder for brevgiro. Dette gjelder for det første det faktum at kunden må håndskrive nødvendig betalingsinformasjon. Dette må antas å innebære at kunden opplever en større kontroll med hva som nedskrives og undersøker dette på en mer omstendelig måte. For det andre må ikke kunden forholde seg til andre faktorer av systemteknisk art, slik som passord, engangskoder, annen brukerlegitimasjon og sikkerhetsverktøy. For det tredje er bruk av de tradisjonelle giroblankettene avtagende. Opplysninger fra BBS viser også at slike tapssituasjoner er av begrenset omfang.

Ved bruk av bankgiro må kunden dessuten vise legitimasjon og påføre sin underskrift for at oppdraget skal kunne sendes til belastning. Dette forholdet må også antas å medføre at kunden blir mer varsom og oppmerksom på betalingsinformasjonen. Selve hendelsesforløpet ved denne giroformen, det vil si å oppsøke en bankfilial, sette seg ned hos en bankfunksjonær og vise legitimasjon og underskrive på betalingsoppdraget, bygger opp om dette.

2) Ved bruk av brevgirotjenesten må kunden også selv påføre nødvendig betalingsinformasjon og underskrift. Giroblankettene kan deretter sendes inn til BBS for belastning. Tidsaspektet, det vil si fra kunden nedtegner nødvendig betalingsinformasjon og sender blankettene per post, er et viktig forhold av betydning her. Kunden må antas å få flere anledninger til å dobbeltsjekke at riktig betalingsinformasjon er påtegnet.

Reglene om tilbakekall, jf. avsnitt 2.5 foran, kan heller ikke sies å være utilstrekkelig for bank- og brevgiro. For brevgiro er tilbakekallsmuligheten i visse tilfeller noe begrenset, men dette må anses som en konsekvens av dette systemet, jf. avsnitt 3.3.2 foran. *Banklovkommisjonen* kan heller ikke se at reglene om avtaleinngåelse, oversikt over konto mv. i finansavtaleloven, kan anses utilstrekkelig eller mangelfulle i forhold til tap som er oppstått som følge av kundens egne feil. Etter *Banklovkommisjonens* oppfatning taler disse forhold for at tap som følge av feiloverføringer ved bruk av bank- eller brevgiro bør påhvile den enkelt kunde. Som nevnt i avsnitt 3.3.3 har *Banklovkommisjonen* videre vurdert de potensielle tapssituasjonene ved bruk av ferdigutfylte blanketter og belastningsgiro som svært liten. *Banklovkommisjonen* har derfor lagt til grunn at det heller ikke for disse giroformene er nødvendig med en nærmere lovregulering.

3.5.2 Andres misbruk

1) For giro som innleveres i en bankfilial, vil misbrukssituasjonene som oftest være av en slik karakter at det vanskelig kan tenkes at kunden har opptrådt grovt uaktsomt. Det krever enten tilegnelse av kundens legitimasjonskort eller tilstrekkelig informasjon til å lage et falskt legitimasjonskort, samt påtegning av falsk underskrift. Risikoen for tapssituasjoner i slike tilfeller må derfor for det første anses som forholdsvis begrenset. For det andre vil gjeldende ansvarsregulering i finansavtaleloven § 34 i de fleste tilfeller medføre at kunden holdes skadesløs. Her må det for så vidt tas forbehold for de tilfeller hvor kunden svikaktig har medvirket til den urettmessige belastningen, jf. finansavtaleloven § 34 fjerde ledd. Slike tilfeller er for så vidt sjeldne. Ifølge statistikk fra BBS har det kun forekommet tre oppdagete svindelhendelser siden 2003.

2) For brevgirotjenesten er det skilt mellom de tilfeller hvor misbruk skjer av utenforstående eller av medlemmer i kundens husstand. I de førstnevnte tilfellene kan det vanskelig tenkes typetilfeller hvor kunden kan sies å ha opptrådt grovt uaktsomt. Det kan nok forekomme tilfeller hvor kunden ikke har oppbevart følgesedlene på en sikkerhetsmessig måte. Dette har imidlertid liten betydning så lenge betalingsoverføringene er forutsatt av at kunden undertegner følgesedlene. Dersom det først er påtegnet falsk underskrift, kan det ikke sies at kunden har opptrådt grovt uaktsomt. Også her må det imidlertid tas forbehold for de tilfeller hvor kunden forsettlig har medvirket til den urettmessige belastningen, jf. finansavtaleloven § 34 fjerde ledd.

I de tilfeller hvor noen av kundens nærstående har fått tak i følgesedlene og påført falsk underskrift, kan det også vanskelig sies å foreligge grov uaktsomhet. Dette må antas å gjelde selv om risikoen for at slikt misbruk kan forekomme er større enn vanlig. *Banklovkommisjonen* finner i denne forbindelse grunn til å vise til Bankklagenemndas sak BKN-97050. Her hadde en fostersønn til kunden urettmessig belastet kundens konto ved hjelp

av falske fullmakter. I vurderingen av om kunden hadde opptrådt grovt uaktsomt, ble det ikke lagt vekt på at kunden burde varslet om fostersønnens tidligere tyveri fra hennes safe og misbruk med kort i en annen bank. For å unngå at tapet blir liggende på institusjonens hånd, har BBS imidlertid opplyst om at alle forhold politianmeldes uavhengig av tredjemanns tilknytning til kunden. Som nevnt i avsnitt 3.4.1 foran, vil kunden i de fleste tilfeller velge å ikke forfølge saken, slik at tapet til syvende sist vil kunne bli liggende hos kunden. Dette forholdet gir, etter *Banklovkommisjonens* mening, imidlertid ikke et tilstrekkelig grunnlag til å foreslå en nærmere ansvarsregulering med sikte på å begrense slike potensielle tapssituasjoner.

De nåværende reglene i finansavtaleloven etterlater, etter *Banklovkommisjonens* oppfatning, heller ikke her et behov for en nærmere regulering. I denne sammenheng nevnes at finansavtalelovens regler om oversikt over konto, jf. avsnitt 2.3.1, gir kunden en grei kontroll over sine betalingsoverføringer. Banklovkommisjonen nevner videre at reglene om misbruk i lovens § 34 også ble vurdert og foreslått på et tidspunkt hvor bankgiro mv. var en av de viktigste formene for betalingsoverføring, slik at risikospørsmål og egnet regulering for slik overføring må anses som forholdsvis bra tilpasset for disse. *Banklovkommisjonen* har slik sett vurdert reglene for de ulike girotjenestene som tilfredsstillende, og ser heller ikke her et behov for en nærmere lovregulering på dette området.

I det følgende er således betalingsoverføringer ved bruk av giro utelatt, og *Banklovkommisjonen* har ikke funnet grunn til å foreslå ytterligere regulering av slike betalingstjenester. *Banklovkommisjonen* finner imidlertid grunn til å nevne at girobetalinger som gjøres over et nettbasert system, drøftes nærmere i kapittel 5 nedenfor. Dette gjelder vanlige overføringer til privatpersoner, overføring ved hjelp av ferdigutfylte blanketter, ofte i form av eFaktura, og belastningsfullmakter. Når det gjelder de to sistnevnte formene for overføring nevner *Banklovkommisjonen* allerede her at risikobildet for slike belastningsformer i stor grad er samsvarende med det som er redegjort for i dette kapitlet.

Kapittel 4
Betalingsoverføring ved bruk av debet- og kredittkort

4.1 Innledning

Betalingsoverføringer knyttet til kontantuttak og handel (kjøp av varer og tjenester), gjennomføres på nåværende tidspunkt i stor grad ved bruk av betalingskort, både kreditt- og debetkort. Ifølge tall fra Norges Bank, var det ved utgangen av 2007 utstedet ca. 9,3 millioner betalingskort i Norge.[1] 3 millioner av disse er rene kredittkort. 4,8 millioner er såkalte kombinerte kort som inneholder både en debet- og kredittkorttjeneste.[2] Hver innbygger i Norge betalte gjennomsnittlig 207 ganger med kort i 2007.[3] Dette innebærer et totalt transaksjonsvolum for bruk av betalingskort på ca. 967 millioner.[4] Det er 13 prosent mer enn i 2006, og innbyggerne bruker betalingskort ved en større del av handlene enn tidligere. Kortbaserte betalingstjenester er en uensartet gruppe tjenester som i utgangspunktet ikke har mer til felles enn at man gjør bruk av et plastkort. Kortene benyttes både til elektroniske og papirbaserte systemer. For de førstnevnte elektroniske systemene gjennomføres belastningen som oftest ved inntasting av PIN-kode, mens for de papirbaserte systemene forutsetter belastningen at kunden undertegner manuelt. Plastkortet fungerer som en «nøkkel» til et bredt spekter av betalings- og kredittjenester.

Ser man på oppgjørsformen mellom kunden eller korthaver og kortselskap (utsteder), kan man dele betalingskortene inn i forskjellige hovedgrupper. For det første kan kunden benytte seg av *debetkort*. Disse kortene er knyttet til en innskuddskonto, og representerer en av de vanligste formene for betalingskort undertiden. Kortet benyttes her til å disponere over det som til enhver tid er disponibelt på kontoen. Eksempler på debetkort i Norge er først og fremst bankenes betalingskort. Banker i Norge har et samordnet kortsystem. Dette innebærer at alle kort som er utstedt av bank og som omfattes av det felles regelverk, kan benyttes i alle betalingsterminaler og/eller minibanker som inngår i samordningen. Dette kortsystemet kalles for «BankAxept». Per 2005 fantes det om lag 100 000 rene BankAxept-kort.[5] I tillegg kan kunden benytte seg av VISA-kort, som i utgangspunktet er et internasjonalt debetkortsystem. Det er imidlertid opp til utsteder av disse kortene, det vil si de fleste norske bankinstitusjoner, om det også skal være mulig å benytte det som et kredittkort, jf. avsnittet foran. Norske banker utsteder ofte betalingskort som kombinerer funksjonene til BankAxept og VISA. Den internasjonale tilknytningen, medfører at kunden med slike kort kan foreta betalinger og uttak også i utlandet.

For det andre er det mulig å benytte seg av *kredittkort*. Disse kortene inndeles vanligvis i to kategorier. Ved den ene typen kredittkort får kortholderen innvilget en *kontokreditt* i henhold til en kontokredittavtale som det trekkes på.[6] Kreditten vil være begrenset til et beløp som er avtalt på forhånd, og utnyttet kreditt nedbetales avdragsvis etter en avtalt betalingsplan. Vanlige bankkort kan være tilknyttet slike kontokredittordninger, slik at kortet knyttes til en konto i banken som utsteder kortet. Det eksisterer imidlertid også særskilte kontokredittkort. Eksempler på sistnevnte kredittkort er blant annet VISA, Mastercard, Crescokort, Norwegian-kortet, Kash® Visa-kort, Re:member-kort og Centum Finans-kort. Den andre varianten av kredittkort er *faktureringskort*. Kunden benytter i disse tilfeller kortet ved kjøp av varer og tjenester og utestående mellom kunde, kortselskap og salgssted gjøres opp i etterhånd. Kontohaveren får med jevne mellomrom (30-40 dager) en samlefaktura over kjøp foretatt på kortet og kunden benytter betalingstjenester som for eksempel brevgiro eller nettbank, for å gjøre opp sitt utestående med kortselskapet. I andre tilfeller gjør kontohaveren opp sin gjeld til kortselskapet gjennom avtale om direkte belastning av kontohavers konto i bank. Ved bruk av faktureringskort får kontohaveren en betalingsutsettelse (kreditt). Eksempler på faktu-

[1] Norges Banks årsrapport om betalingssystem 2007 side 45.
[2] Se også NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.2.4.
[3] Norges Banks årsrapport om betalingssystem 2007.
[4] Norges Banks årsrapport om betalingssystem 2007 side 46.
[5] Jf. NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.2.4.
[6] Se Banklovkommisjonens utredning nr. 17 (NOU 2007: 5) Frarådingsplikt i kredittkjøp avsnitt 5.3.1 om en vurdering av slike avtaler.

reringskort er American Express og Diners Club, selv om disse også ofte benyttes som vanlige kontokredittkort.

For det tredje kan kunden benytte seg av såkalte *forhåndsbetalte kort*. Her er kjøpekraften lagret i selve kortet og er ikke knyttet til en bakenforliggende konto. Kjøpekraften er nominert i penger, og klippes ned etter hvert som kortet brukes. En skiller her mellom åpne og lukkede systemer. I et lukket system vil en vanligvis bare ha én tilbyder for varer og tjenester, for eksempel kantinekort i større bedrifter eller lignende. I et åpent system vil en ha flere tilbydere, for eksempel ulike transportselskaper osv. En kan også skille mellom ladbare og ikke ladbare kort. En kan tenke seg at ladbare kort kan «etterfylles» med kjøpekraft for eksempel fra en konto. Smartkort er et eksempel på et slikt forhåndsbetalt kort, som for så vidt kan benyttes som ID-kort, adgangskort, gavekort mv. I tillegg til dette kan smartkort også benyttes som vanlige debet- og kredittkort.

Sammenliknet med andre land blir en stor del av korttransaksjonene i Norge utført med debetkort. Det nasjonale debetkortsystemet BankAxept dominerer. Internasjonale betalingskortsystem som VISA og MasterCard har tatt en økende del av markedet de siste årene. Det er ellers fortsatt et stort avvik i bruken mellom debetkort og kredittkort.[7] I det følgende tas det utgangspunkt i disse debet- og kredittkortene.

4.2 Virkemåten

4.2.1 Generelt

Både debet- og kredittkort har tradisjonelt sett hatt to informasjonselementer som har bestått av informasjon på det fysiske kortet og informasjon i magnetstripen. Innholdet av informasjonen i magnetstripen bygger på internasjonale standarder og skal sørge for sikker gjennomføring av betalingstransaksjoner. De norske bankene utsteder for øvrig nå betalingskort med såkalt smartkort- eller EMV-standard. EMV er en teknisk standard for gjennomføring av betalingstransaksjoner i betalingsterminal og minibank, og regulerer kommunikasjonen mellom kortet og terminal, samt de bakenforliggende avregningssystemer. Slike smartkort er utstyrt med en liten databrikke eller chip. Kortene kalles derfor ofte chipkort. Innføringen av slike kort i det norske betalingskortmarkedet er først og fremst begrunnet i ønske om bedre sikkerhet rundt korttransaksjonene. Den økte sikkerheten gjenspeiles særlig i muligheten for PIN- og autorisasjonskontroll også i såkalte «offline»-situasjoner og at det kan legges inn flere individuelle parametre, for eksempel beløpsgrenser. Selv om EMV-standarden innføres på alle betalingskort, herunder debetkortene, vil BankAxept fortsatt fungere parallelt. Med tiden vil imidlertid all informasjon fra magnetstripene bli lagt over på chip, herunder BankAxept-systemet. Kort med chip har naturligvis mye å si i forhold til risikoen for misbruk av betalingskortene, se også avsnitt 4.5 nedenfor.

Flere betalingskort fungerer både som et debet- og kredittkort, slik at kunden fra gang til gang kan velge hvordan belastningen skal gjøres. Dette beskrives nærmere i avsnitt 4.2.2 nedenfor. Det er heller ikke de store forskjellene mellom hvilke steder de forskjellige korttypene kan brukes. Selve belastningsprosessen er imidlertid annerledes og *Banklovkommisjonen* har derfor funnet det hensiktsmessig å dele opp den følgende fremstillingen av betalingskortenes virkemåte etter bruk av debetkort, jf. avsnitt 4.2.2, og bruk av kredittkort, jf. avsnitt 4.2.3. Den ulike belastnings- og avregningsprosessen vil særlig ha betydning i forhold til risikoen for feilbruk av betalingskortet. I redegjørelsen av risikoen for kundens egne feil er derfor skillet mellom debet- og kredittkort beholdt, se henholdsvis avsnitt 4.3.1 og 4.3.2.

4.2.2 Debetkort

Som nevnt i avsnitt 4.1 foran, er debetkortene knyttet til kundens innskuddskonto. Det vil si at kortene bare kan benyttes som betalingsinstrument så lenge kunden har midler på kontoen. Debetkortene er de vanligste formene for betalingskort i Norge. Det norske kortsystemet er bygget opp som et «online»-system hvor tilhørende kort er merket med «BankAxept»-logoen. Dette innebærer at det i utgangspunktet kun godtas «online»-transaksjoner med PIN-verifikasjon. Belastningen blir da umiddelbart reservert på kundens konto. Det nevnes at slikt oppgjør også gjelder for VISA Electron. I visse tilfeller blir det imidlertid iverksatt reserveløsninger og det er særlig aktuelt ved bruk av salgsterminaler som er beskrevet i avsnittet nedenfor.

Med visse debetkort er det imidlertid også lagt til rette for «offline»-transaksjoner. Slike kort er således tilrettelagt for både en debet- og en kredittfunksjon. Dette er ikke uvanlig for kort utstedt av norske banker. Disse debetkortene er som oftest utstyrt med logo fra VISA eller MasterCard. Det vil

[7] Norges Banks årsrapport om betalingssystem 2007.

imidlertid foregå en elektronisk kommunikasjon mellom salgsterminalen og en driftssentral som er knyttet opp mot kundens bank. Dette er først og fremst en sikkerhet i forhold til kortets kreditt og gyldighet. Det kan således anses som en «online»-autorisasjon med kreditt. Ved selve gjennomføringen av kjøpet, må kunden signere på en kvittering som tjenesteyteren beholder. Selve transaksjonen blir ikke reflektert på kundens konto før opptil flere dager senere. I deler av utelivsbransjen og taxinæringen er dette en vanlig form for oppgjørsmåte. Det kan være begrunnet i at det er mer kostbart med en salgsterminal som støtter BankAxept, men også fordi næringens regnskapssystemer er tilrettelagt for kredittransaksjoner.

Debetkortene har mange bruksområder. For det første kan det benyttes i *minibank* hvor kunden kan ta ut kontanter. Kunden må da innsette betalingskortet i automaten, taste en firesifret PIN-kode, velge uttaksbeløp og bekrefte utbetalingen. For uttak i minibank med debetkort blir beløpet umiddelbart reservert på kortholders konto. Selve transaksjonen til belastning av kortholder bli generert senere. Denne går via en avregningssentral som sørger for at den automateiende banken blir kreditert det beløp som er tatt ut fra kortholders bank. Gebyrene varierer alt etter hva slags kort og minibank kunden benytter seg av. *Banklovkommisjonen* finner ikke grunn til å gå nærmere inn på dette. Flere banker har også innført gebyrfrie uttak i utenlandske minibanker. Enkelte minibanker kan også tilby andre tjenester. Dette er for øvrig ikke samordnede tjenester slik at de ikke nødvendigvis er åpne for kortholdere i andre banker enn automatens eier.

For det andre kan debetkort brukes i forretninger eller lignende som har *salgsstedsterminaler*, såkalt Electronic Funds Transfer at Point of Sale (EFTPOS). Dette kan henspeile seg både på terminaler som står fast og er direkte koblet opp mot et nettverk og såkalte mobile terminaler som kommuniserer via GPRS-nettverket. Betalingsterminaler på brukersteder er knyttet opp mot en driftssentral. Driftsentralen har avtale med brukerstedets bankforbindelse (transaksjonsbank) om å autorisere og samle inn transaksjoner. Dette er på nåværende tidspunkt et utbredt fenomen. Slik kortbetaling innebærer at kunden gjør opp for seg på salgsstedet, enten det dreier seg om kjøp av varer eller tjenester. EFTPOS varekjøp fører til at beløpet umiddelbart reserveres på kortholders konto. Selve transaksjonen til belastning av kortholder blir generert senere, på samme vis som ved uttak i minibank. Denne går via en avregningssentral som sørger for at det blir generert kredittransaksjoner til brukerstedet.

Som vist foran, er det norske debetkortsystemet i utgangspunktet et system hvor det er «online» kontakt mellom kortet og driftsentralen. Det er imidlertid ikke uvanlig at det ikke oppnås kontakt mellom terminal på brukersted og bank eller datasentral som mottar transaksjoner. Dette gjelder særlig for de mobile salgsterminalene. Da iverksettes en reserveløsning. I reserveløsningen må kortholder legitimere seg og signere en kvittering der deler av kontonummeret og transaksjonsbeløp er fylt ut. Brukerstedet er forpliktet til å sjekke kortholders legitimasjon. Transaksjonsbanken skal besørge at transaksjoner dannet på grunnlag av reserveløsningen, blir overført til kontobank. Reserveløsning kan for så vidt ikke benyttes for beløp over 1.500 kroner ved elektronisk reserveløsning og er kun gyldig inntil seks timer. Dette følger av BankAxept-reglene som brukerstedet må akseptere for å kunne benytte seg av terminalen. Det er således ikke tenkt som en langvarig beredskapsløsning eller som en kredittfunksjon for kortholderen. For høyere beløp enn 1.500 kroner må brukerstedet ringe inn til BBS for en såkalt dekningskontroll og motta en autorisasjonskode som skal brukes for slike belastninger. Kundens medvirkning er for så vidt ikke avvikende i slike tilfeller, det vil si at det kun kreves legitimering og påtegning av underskrift på den utskrevne kvitteringen. Kvitteringen må sendes til BBS for manuell belastning av kortholders konto.

Ved bruk av salgsstedsterminaler må kortholder i visse situasjoner inntaste eller nedskrive totalbeløpet selv, typisk i forbindelse med et restaurant- eller baropphold. For slike transaksjoner er det mer og mer vanlig at kortholder inntaster PIN-kode, det vil si at debetkort med «BankAxept»-logoen kan benyttes. Manuell nedskrivning av totalbeløp kan også forekomme ved visse debetkort. Som vist foran krever dette imidlertid at debetkortet er utstyrt med VISA- eller MasterCard-logo.

I de fleste forretninger eller lignende med betalingsterminal, særlig dagligvareforretningene, er det også lagt til rette for kontantforsyning via cash-back og cash-out. Dette vil si at man ber forretningen om å debitere kontoen for et høyere beløp enn varekjøpet og får differansen i kontanter. Betalingskort som brukes i salgsstedsterminaler, innebærer at forretningen inntaster et beløp som skal gjenspeile kostnaden for varen eller tjenesten, eventuelt med et tillegg som kunden ønsker å ta ut i kontanter.

I 2005 utviklet bankene i fellesskap en ny norskbasert debiteringstjeneste til bruk ved handel over Internett, såkalt «BankAxess». Dette innebærer at kjøperen foretar betalingen direkte fra egen konto uten å gi fra seg kortopplysninger. Kunden legitimerer seg og godkjenner betalingen ved bruk av BankID, se punkt 5.2.1 punkt 2) nedenfor for mer om dette identifikasjonssystemet. Etter hvert vil BankAxess også kunne brukes i forbindelse med andre former for netthandel, for eksempel via mobiltelefon og digital-TV. Handel over Internett kan imidlertid også gjøres med betalingskort, særlig med kredittkortene, se avsnitt 4.2.3 nedenfor. Dette er ikke mulig med de norske debetkortene, det vil si kort merket med «BankAxept» og er en av grunnene til at debiteringstjenesten «BankAxess» er utviklet.

4.2.3 Kredittkort

Som nevnt i avsnitt 4.2.1 foran, er bruksområdene for debet- og kredittkort forholdsvis sammenfallende. Det som skiller kortene fra hverandre er særlig oppgjørssystemet, det vil si tidsaspektet på transaksjonene og gebyrer som ilegges for bruken. Avhengig av hva slags betalings- eller uttakspunkter som kortholder benytter seg av, kan transaksjonene som oftest enten gjennomføres ved hjelp av PIN-kode eller ved å signere kvittering for det aktuelle transaksjonsbeløpet. Belastningene som utføres på denne måten, regnes ikke opp mot kortholders private konto, men mot en opprettet konto med en kredittgrense som er avtalt med kortutsteder. Transaksjonene er således ikke knyttet opp til penger som kortholder besitter, men til penger som kortholder låner og periodevis betaler tilbake. Som vanlig vil kortholder en gang i måneden motta en oversikt over de transaksjoner som er gjort og det totale beløpet som skal innbetales til kredittkortselskapet. Til flere kredittkort er det knyttet flere fordeler. Dette kan være gunstige reise- og avbestillingsforsikringer, rentefri kreditt i et visst tidsrom eller poeng eller lignende som på et gitt tidspunkt vil gi kortholder rabattert pris på tjeneste eller vare.

Ved uttak i minibank må kortholder gå frem på samme måte som ved bruk av debetkort. Beløpet som er disponibelt for uttak regnes opp mot kredittkortets kredittgrense for den aktuelle perioden. Uttaket er imidlertid normalt gjenstand for et gebyr som ofte vil tilsvare en prosentvis andel av det samlede uttaket.[8]

Kredittkortene kan brukes i salgsstedsterminaler og har et større bruksområde enn de norske debetkortene. Betalingskort merket med «BankAxept»-logoen kan bare brukes på salgsterminaler som støtter et «online»-system, noe som ikke er en betingelse for bruk av kredittkortene. Som vist i avsnitt 4.2.2 foran, er det imidlertid ikke uvanlig at de norske debetkortene også er utstyrt med eksempelvis VISA-logoen, slik at disse også kan brukes i betalingsterminaler som ikke nødvendigvis er «online».

Kredittkortholderen kan videre benytte sitt betalingskort ved handel over Internett. Som vist i avsnitt 4.2.2 foran, kan ikke dette gjøres med de norske bankkortene. Imidlertid er et stort antall av betalingskortene som er utstedt av norske banker knyttet opp til internasjonale kortselskaper som VISA eller Mastercard slik at de norske kundene likevel har hatt mulighet til å handle over nettet.[9] Det norske kontonummeret kan uansett ikke brukes for belastning på Internett ved kjøp av varer eller informasjon, ettersom det går via et annet kortsystem. Ved slik elektronisk handel må kunden inntaste navnet på kortholder (fremgår som oftest av kortet), kortnummeret som vanligvis står på forsiden av det fysiske kortet, utløpsdato for kortet, samt inntaste en autorisasjonskode på tre siffer. Sistnevnte er en såkalt sikkerhetsverdi som skal kontrolleres for å verifisere at kortet er ekte. Denne koden kalles enten for CVC (Card Verification Code), men er også kjent som CVC2 eller CVV2 avhengig av kortutsteders system. Banklovkommisjonen nevner at VISA har lansert en ny og mer sikker tjeneste for handel over Internett, såkalt «Verified by Visa». Løsningen sørger for at partene, kortholder og nettbutikk, blir autentisert overfor den andre parten. Flere av bankinstitusjonene som utsteder VISA-kort i Norge tilbyr denne tjenesten. I tillegg til å oppgi kortnummer og utløpsdato, må brukeren identifisere seg med en selvvalgt kode eller kode mottatt fra kortutsteder.

4.3 Risiko for kundens egne feil

4.3.1 Debetkort

Bruk av debetkort er som vist foran, knyttet direkte opp mot uttak av kontanter eller kjøp av varer og/eller tjenester. Dette innebærer at kun-

[8] I oppgjøret av internasjonale betalingskortene involveres langt flere aktører. Det har særlig blitt stilt spørsmålstegn ved de ulike formidlingsgebyrene. I desember 2007 vedtok for så vidt EU-kommisjonen at MasterCard ikke kan kreve formidlingsgebyr på grensekryssende betalinger innenfor EØS-området. I mars 2008 åpnet EU-kommisjonen også en sak mot VISA Europa. Finansdepartementet har ellers bedt Konkurransetilsynet i Norge om å vurdere formidlingsgebyret og brukerstedsgebyrene etter konkurranseloven.

[9] Med unntak av VISA Electron.

dens medvirkning til at transaksjonen gjennomføres er av begrenset karakter, slik at risikoen for feiloverføringer eller lignende og potensielle tapssituasjoner er lav.

Ved bruk av minibank, må kunden inntaste kode og velge ønsket beløp før uttaket gjennomføres. Dersom kunden taster feil kode, mottar han eller hun en feilmelding, og transaksjonen vil ikke bli gjennomført. Det kan for så vidt forekomme tilfeller hvor kunden velger feil beløp. Dette medfører imidlertid kun at kunden tar imot et lavere eller høyere beløp enn ønsket. Kontantene skyves ut samtidig, slik at risikoen for at kunden kun tar med opprinnelig ønsket beløp og etterlater det overskytende, må anses som svært liten. Ved såkalt cash-back og cash-out i dagligvareforretninger, jf. avsnitt 4.2.2 foran, er det imidlertid en risiko for at kunden ikke oppdager at mottatt beløp ikke samsvarer med den faktiske belastningen av kontoen.

Ved kjøp av varer og tjenester, må det skilles mellom de tilfeller hvor det på forhånd er fastslått et totalbeløp og de tilfeller hvor kunden må taste inn slikt beløp selv for å deretter å taste inn PIN-koden.

De førstnevnte situasjonene vedrører særlig bruk av salgsterminaler, hvor transaksjonen er knyttet opp til et fastsatt forhåndsbestemt gjeldsforhold mellom utsalgsstedet og kunden, typisk vareprisen. Dette innebærer at kundens medvirkning består i å godkjenne gjeldsforholdet ved inntasting av PIN-kode. Sannsynlige feilkilder i slike situasjoner vil typisk være at kunden taster inn feil PIN-kode. Konsekvensen av slik feilinntasting er imidlertid at kunden mottar en feilmelding og at transaksjonen ikke gjennomføres. Dersom det må iverksettes en reserveløsning og kortholder må påføre sin underskrift, kan det imidlertid vanskelig tenkes å oppstå situasjoner hvor kjøpet ikke blir gjennomført. En annen mulighet er dessuten at brukerstedet taster inn for høyt beløp og kunden feilaktig godkjenner dette ved PIN-verifikasjon.

I de situasjoner hvor kunden må taste inn totalbeløp selv, er risikoen for at det oppstår tapssituasjoner som følge av kundens feil, større. Dette er først og fremst aktuelt ved bruk av salgsterminaler, gjerne i tilknytning til en eller annen form for serviceyting. Her er ikke totalbeløpet fastslått på forhånd og feiltasting av tilsiktet beløp på terminalen, kan medføre at kortholders konto blir belastet i et større omfang enn det kunden ønsker. Dette kan i visse tilfeller forsterkes av den situasjon kunden befinner seg, for eksempel ved at det er mørkt barlokale og kunden er beruset.

4.3.2 Kredittkort

Kredittkortene har som vist i avsnitt 4.2.3 foran forholdsvis likt bruksområde som debetkortene. Visse forskjeller er det imidlertid, blant annet muligheten til å handle over Internett. Risikoaspekter knyttet til slik handel kommenteres til slutt i dette avsnittet. Så lenge kredittkortet benyttes ved hjelp av PIN-kode, vil risikobildet være tilsvarende som angitt i avsnitt 4.3.1 foran. For slike kredittkorttransaksjoner vises det derfor til denne beskrivelsen.

Når det gjelder bruk av kredittkort på salgsstedsterminaler, er slike transaksjoner, som nevnt i beskrivelsen av kredittkortenes virkemåte i avsnitt 4.2.3 foran, ikke betinget av at terminalen støtter et «online»-system. Slik sett er det lagt opp til at kortholderen kan underskrive på kvitteringen på det aktuelle beløpet, uten at dette er å anse som en reserveløsning som ved debetkortene. Her må det også skilles mellom de situasjoner hvor kortholder kun trenger å verifisere kjøpsbeløpet ved hjelp av sin underskrift og de situasjoner hvor ekstrabeløp og totalbeløp må påtegnes før vedkommende underskriver på transaksjonen.

I de førstnevnte situasjonene kan det vanskelig tenkes å oppstå tapssituasjoner. Imidlertid kan det forekomme tilfeller hvor kredittkortholderen underskriver på et for høyt beløp i forhold til det som var avtalt eller uttrykkelig fremkom av prisen på varen eller tjenesten. Dette er imidlertid en risiko som elimineres i stor grad av gjeldende betingelser for bruk av kortet. Dette er gjennomgått i avsnitt 4.4 nedenfor.

Når det gjelder de situasjoner hvor kortholderen selv må påtegne totalbeløpet, kan det på samme vis som ved bruk av debetkortene, forekomme feil. Dette vil særlig kunne manifestere seg i feilaktig nedskriving av totalbeløp, for eksempel en null for mye. Det må antas at det er lettere å gjøre feil ved manuell påtegning enn inntasting på en betalingsterminal som ved debetkortene. Håndskrevne tall kan dessuten lettere misoppfattes av brukerstedet slik at feil beløp innrapporteres til belastning av kortholders kredittkonto. Muligheten for å oppdage slike feil er også vanskeligere ved bruk av kredittkort, ettersom transaksjonen ved de regulære kredittkortene ikke vises like raskt som ved debetkortene. En oversikt over transaksjonene kan komme en stund etter at transaksjonen ble gjort, slik at kortholderen, ved mindre beløpsavvik, kan bli usikker på om det er en riktig belastning eller ikke.

Ved bruk av kredittkort over Internett, nevnes det at kunden må medvirke på et høyere nivå enn

ved bruk av betalingsterminaler. Kunden må i slike tilfeller, som nevnt i avsnitt 4.2.3 foran, taste inn en del informasjon, og det kan ikke utelukkes at det forekommer feil i slike tilfeller, for eksempel feil angivelse av kortnummer osv. Resultatet ved slik feiltasting er likevel at belastningen ikke utføres. Sannsynligheten for at slik feiltasting – sett i sammenheng med krav om inntasting av det fysiske kortets CVC-kode – skal medføre at kunden belaster kortet til en annen kunde, må også anses som ikke-eksisterende. Dette ville uansett ikke medført noe økonomisk tap for kunden, og er heller et aktuelt spørsmål i forhold til risiko for andres misbruk, se avsnitt 4.5 nedenfor.

4.4 Ansvarsregulering ved kundens egne feil

Risikoen for at det skal forekomme tapssituasjoner som følge av kundens egne feil ved bruk av betalingskort, er som vist i avsnitt 4.3 foran, av begrenset karakter. I de tilfeller hvor kunden selv må påføre (ved inntasting eller håndskrift) totalbeløpet, kan imidlertid dette medføre større tap for kunden. I det følgende er det ikke foretatt et skille mellom debet- og kredittkortene. Dette er særlig begrunnet i at avtalevilkårene for de to korttypene langt på vei er samsvarende og at aktuelle bestemmelser i finansavtaleloven ikke skiller mellom debet- og kredittkort. Visse forskjeller er det imidlertid og er kommentert nedenfor.

1) I avtalevilkårene for bruk av betalingskort, er feilbelastninger i forbindelse med kjøp av varer og tjenester regulert nærmere. Dette omhandler i første rekke betalingskort generelt, det vil si vanlige bankkort som BankAxept, samt andre kredittkort. I den utstrekning kontohaveren bestrider å ha ansvar for en belastning ved bruk av betalingskort, skal banken tilbakeføre beløpet og erstatte rentetapet fra belastningstidspunktet. Dette er først og fremst aktuelt ved misbrukstilfellene, ettersom loven krever at kontohaveren ikke har erkjent ansvar for belastningen, se finansavtaleloven § 37 og avsnitt 2.6.5 foran.

I avtalevilkårene er det imidlertid forutsatt at slik tilbakeføring også skal skje i andre situasjoner, det vil si hvor kunden har godkjent belastningen, men hevder at det ble gjort ved en feiltakelse. I noen avtalevilkår er dette antitetisk formulert som at tilbakeføringsplikten ikke gjelder feilregistreringer på brukerstedet som kontohaver selv burde ha oppdaget ved bruk av kortet i forbindelse med betalingen for varen eller tjenesten. I de fleste tilfeller vil det nok være klart at kontohaveren burde oppdaget dette, for eksempel ved at det ble påført en ekstra null ved inntasting eller nedskriving av totalbeløp på en restaurant, men det kan ikke utelukkes tilfeller hvor kunden likevel må sies å ha opptrådt med tilstrekkelig aktsomhet. Dette må for øvrig sees i sammenheng med at avtalevilkårene bestemmer at salgsnotaer skal oppbevares for senere eventuell kontroll mot transaksjonsoversikten, enten via postsending eller som kontooversikt via nettbaserte betalingstjenester. I avtalevilkårene er det bestemt at reklamasjoner om slike forhold må rettes mot brukerstedet. Det er dessuten stor sannsynlighet for at brukerstedet vil ta reklamasjonen til følge, av hensyn til for eksempel risiko for dårlig omdømme eller publisitet i media mv. Dette vil imidlertid ikke gjelde i like stor grad i forhold til kortbruk i utenlandske salgs- eller servicesteder, særlig ikke dersom det gjelder varer og tjenester av tvilsom art, for eksempel strippeklubb eller lignende. Dersom kontohaveren reklamerer til brukerstedet, kan vedkommende uansett velge å fremme reklamasjon mot institusjonen, jf. kredittkjøpsloven § 8. Dette er også eksplisitt kommet til uttrykk i standardvilkårene for kredittkort.

Når det gjelder kredittkort, er det fastslått særlige reklamasjonsregler. Ved eventuell feilbelastning av transaksjoner må kortholder reklamere overfor banken omgående og ikke senere enn fastsatte frister (normalt 30 dager) etter at transaksjonsinformasjonen er gjort tilgjengelig. I noen av avtalevilkårene er det videre fastslått at selv om reklamasjonsfristen er overskredet, vil banken forsøke å få feilen rettet opp, men påtar seg ikke noe ansvar i denne forbindelse.

Reglene i kontoavtalen innebærer således en viss mulighet for kontohaver til å få eventuelle feilbelastninger gjenopprettet. En nærmere vurdering av behovet for lovregulering for slike feilbelastninger er gitt i avsnitt 4.6 nedenfor.

2) Bortsett fra de nevnte reglene i kredittkjøpsloven om reklamasjon er ikke tap som har oppstått som følge av feilbruk regulert nærmere i lovgivningen. Det forhold at risikoen for oppståtte tapssituasjoner er av begrenset karakter, må i dette henseende antas å være en av grunnene for dette. I Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) ble det også bare foreslått regler om feilaktig godskriving og belastning av en kundes konto, jf. finansavtaleloven §§ 31 og 32. Disse vedrører kun feil fra institusjonens side. På side 141-142 i utredningen, ble det, som nevnt i avsnitt 2.4 foran, presisert at bestemmelsene ikke gjelder dersom det er andre enn banken selv eller dennes medhjelpere som har initiert transaksjonen. Etter gjeldende lovregler er derfor

utgangspunktet at ansvar for tap som følge av feil fra kundens side pålegges kunden selv.

4.5 Andres misbruk

Den mest nærliggende og potensielle tapssituasjonen ved bruk av betalingskort, er andres misbruk. Betalingskort og belastning av konto forutsetter normalt sett kun en form for brukerlegitimasjon. For debetkortene vil dette enten skje ved inntasting av PIN-kode eller signering på kvittering dersom det ikke oppnås kommunikasjon mellom en salgsterminal og driftssentralen. For kredittkortene gjøres dette enten ved inntasting av PIN-kode eller ved signering på kvittering. Kredittkortene kan også benyttes på Internett og brukerlegitimasjonen gjøres da ved at det gis ulike opplysninger som fremkommer av det fysiske kortet. Det kan slik sett forekomme misbruk ved urettmessig tilegnelse av betalingskortet og/eller nødvendig brukerlegitimasjon for å gjennomføre transaksjonen.[10] I 2007 ble det registrert 9 688 sviktaktige transaksjoner med betalingskort. Dette er forholdsvis lavt i internasjonal sammenheng og utgjør rundt 0,3 promille av den samlede omsetningen med betalingskort.[11]

Andres misbruk av betalingskort kan forekomme på forskjellige vis. Tredjemann kan for det første tilegne seg det fysiske kortet, men ikke kode. I slike tilfeller kan vedkommende belaste kortet i salgsterminaler hvor det ikke kreves inntasting av PIN-kode, noe som er særlig aktuelt for kredittkortenes del. Dette fordrer for øvrig at brukerstedet ikke krever å se legitimasjon eller at tredjemann har forfalsket nødvendig legitimasjon. Etter standardvilkårene for bruk av kredittkort, trengs legitimasjon bare å fremvises på anmodning.

For det andre kan tredjemann tilegne seg både det fysiske kortet og PIN-kode. Slik sett kan vedkommende benytte seg av kortet som om det var hans eget, og foreta belastninger i både salgsterminaler med PIN-kode og kontantuttak i minibank, det være seg debet- eller kredittkort. Når det gjelder debetkortene, har disse som oftest et lavere disponibelt beløp enn kredittkortene, slik at tapsomfanget kan bli betraktelig større ved slikt misbruk for en kredittkortholder enn en debetkortholder.

For det tredje kan misbruk være foranlediget av «skimming», det vil si kopiering av det fysiske kortet og magnetstripen. Slikt misbruk har ofte blitt gjennomført ved at tredjemann setter opp fiktive minibanker, enten selvstendige eller som et påbygg til etablerte minibanker, og registrerer kortinformasjonen når kunden setter dette inn. «Skimming» kan også forekomme ved at en utro tjener ved for eksempel en restaurant, særlig i utlandet, tar med seg kortet for belastning og kopierer kortet før det leveres tilbake. Den siste tiden har det også vært eksempler på databaseinnbrudd hos kortleverandørene. De norske bankene utsteder imidlertid nå kort med chip for å redusere slik svindel. Det er vanskeligere å kopiere informasjon i chip enn i magnetstripe, og løsningen er ansett som sikrere. Ved utgangen av 2007 hadde nærmere 30 prosent av bankkortene, det vil si kort med «BankAxept»-logo, chip.[12] I løpet av 2011 skal alle bankterminaler være oppgraderte i forhold til betalingskort med slik chip.

Banklovkommisjonen har ikke funnet grunn til å gå i nærmere detalj om de ovennevnte typetilfellene av andres misbruk av betalingskort. Sikkerhetsrutiner i forhold til verifikasjon av PIN, kryptografiske kontroller mv., er således utelatt. Dette henger særlig sammen med det regelsett som er utformet i forhold til andres misbruk av betalingskort, jf. finansavtaleloven §§ 35 flg. Disse reglene gir en balansert og hensiktsmessig tapsbegrensning for kundens del og er gjennomgått i avsnitt 2.6.3 foran. Se for så vidt avsnitt 4.6 nedenfor om drøftelsen av lovgivningsbehovet.

4.6 Lovgivningsbehovet

1) I avsnitt 4.3 og 4.4 er det gitt en beskrivelse av risiko for og ansvarsregulering ved tap som oppstår som følge av kundens egne feil. Som nevnt må imidlertid risikoen for slike feil anses å være av forholdsvis begrenset karakter. Slik *Banklovkommisjonen* har vurdert det, er det bare i de tilfeller hvor kunden selv må taste inn totalbeløp at det kan forekomme reelle tapssituasjoner. I henhold til avtalevilkårene for betalingskortet, er det imidlertid mulig å reklamere på slike feilbelastninger. Så lenge det er klart at kunden ikke hadde noen grunn til å oppdage det aktuelle forholdet, er det lagt opp til en tilbakeføringsmulighet. Dersom kunden burde oppdaget feilen, er imidlertid ikke dette like klart. Som nevnt i avsnitt 4.4 foran – forutsatt at det dreier seg om en transaksjon som innly-

[10] Når det gjelder handel over Internett, nevner Banklovkommisjonen at tjenestene «BankAxess» og «Verified by Visa» reduserer risikoen for andres misbruk betydelig, se avsnitt 4.2.2. og 4.2.3 foran.

[11] Norges Banks årsrapport om betalingssystem 2007 side 8.

[12] Norges Banks årsrapport om betalingssystem 2007 side 8.

sende er utilsiktet – vil imidlertid brukerstedet som oftest sørge for at feilen korrigeres og at tapet elimineres av hensyn til eget omdømme osv. Selv om reklamasjonsfristene er overskredet, er det videre vanlig at banken forsøker å korrigere feilen. Dette fremgår av noen av bankenes avtalevilkår for betalingskort, se også avsnitt 4.4 foran.

Etter *Banklovkommisjonens* oppfatning er det ikke grunn til å foreslå en nærmere regulering av tapssituasjonene som oppstår på grunn av kundens feilbruk. De vilkårene som foreligger, antas å være rimelige og innebærer en balansert løsning i forhold til krav til korthaverens aktpågivenhet ved bruk av betalingskort, samt muligheten til å få korrigert feilbelastninger i særskilte tilfeller. Så vidt *Banklovkommisjonen* er kjent med, har disse reglene fungert godt i forhold til betalingskortene og en ser ikke behov for å foreslå noen endringer her. *Banklovkommisjonen* finner videre grunn til å nevne at finansavtalelovens regler om oversikt over konto mv., gir kunden en grei kontroll med at transaksjoner har foregått på riktig vis. Denne kontrollen forsterkes dersom kortet er knyttet opp til en nettbankkonto hvor kunden til enhver tid kan undersøke sine utførte betalingsoverføringer. Finansavtalelovens regler om avtaleinngåelse av kontoavtaler, som ofte vil være knyttet opp til kundens betalingskort, må også anses tilfredsstillende og gir lite rom for at kunden i denne prosessen gjør en feil som kan medføre et økonomisk tap, se avsnitt 2.2 foran.

2) Risikoen for tap som følge av andres misbruk av betalingskort er større enn kundens feilbruk. Sikkerheten rundt betalingskortene er imidlertid blitt forbedret, og forbedres stadig blant annet som følge av det nye systemet med chip. Det er dessuten fastslått særlige lovbestemmelser vedrørende slikt misbruk, se avsnitt 2.6.3 foran. Etter *Banklovkommisjonens* oppfatning representerer disse reglene en tilfredsstillende løsning for andres misbruk. De totale kostnadene for misbrukstilfellene er pulverisert i systemet og medfører at kundens egenandel er begrenset på en hensiktsmessig måte.

Banklovkommisjonen er således av den oppfatning at det heller ikke er nødvendig å foreslå noen endringer i reglene om andres misbruk av betalingskort.

Kapittel 5
Nettbasert betalingsoverføring

5.1 Innledning

I Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag), ble det blant annet gitt en oversikt over et stort antall betalingstjenester og behovet for en nærmere lovregulering i forholdet mellom kunden og institusjonen ved bruk av instrumenter for betalingsoverføring. I merknadene til finansavtaleloven § 12 bokstav c) om betalingsinstrumenter, uttalte Banklovkommisjonen, på side 109 i utredningen, at eksempler på betalingsinstrumenter kan være sjekk, giroblanketter, betalingskort med eller uten kode, eventuelt i kombinasjon med terminaler som gir tilgang til betalings- eller kontokortsystemene. Videre at

> «[d]e tradisjonelle betalingsinstrumenter som er nevnt foran, kjennetegnes ved at de utstedes og kontrolleres av kontoførende institusjoner. Utviklingen går nå i retning av at en i økende grad også tar andre særskilte hjelpemidler i bruk, f.eks. telefon, bedriftsterminaler, eventuelt i kombinasjon med koder e.l.
>
> Betalingsinstrumenter representerer et vidt spekter av hjelpemidler som benyttes for å få adgang til betalingsmidler. Slik sett er det ingen prinsipiell forskjell mellom et tradisjonelt betalingsinstrument som giroblankett, og et moderne hjelpemiddel som telefon. Derimot vil ansvar og risikovurderinger kunne bli nokså ulike for instrumenter utstedt og kontrollert av institusjonen, og for hjelpemidler som betaleren selv eller en tredje part er eier av eller ansvarlig for (telefon, terminaler m.v). Dette gjelder særlig i forhold til fremsending av betalingsoppdrag og spørsmål om når og på hvilken måte betalingsoppdrag er kommet frem til institusjonen, jf. spesielle motiver til § 2-31 annet ledd [nå § 39].»

I forhold til de moderne nettbaserte hjelpemidlene, som telefon, var det slik sett spørsmål rundt tid og sted for betaling ved bruk av slike systemer som var hovedtemaet. Risiko- og ansvarsspørsmål i forhold til potensielle tapssituasjoner var ikke sett på som et like nærliggende tema. En grunn til dette var at betalingsoverføringer gjennom elektroniske systemer, bortsett fra betalingskort som det ble foreslått særlige regler for, ikke forutsatte en form for brukerlegitimasjon. På 1990-tallet anså man typiske eksempler på tjenester som effektueres gjennom elektroniske systemer som direkte belastning i form av AutoGiro, direkte remittering (særlig brukt ved masseutbetalinger som lønn og lignende), minibankuttak og EFTPOS transaksjoner. For en nærmere beskrivelse av disse ulike tjenestene vises det til Banklovkommisjonens Utredning nr. 1 side 70 følgende og kapittel 3 og 4 foran.

Betalingsoverføringer skjer imidlertid på nåværende tidspunkt, i tillegg til betalingskort, i stor grad ved hjelp av bankenes nettbanktjeneste og andre nettbaserte overføringsmekanismer, som for eksempel telefonbank. Dette er tjenester eller produkter som er utformet blant annet av hensyn til brukervennlighet og samfunnets økende krav til effektivitet i behandlingen av betalingsoppdrag. Det er således viktig å merke seg at nettbank og telefonbank ikke er et alternativ ved siden av de eksisterende bankinstitusjonene, men tjenester som institusjonene har utformet til eksisterende og potensielle kunder. Slike nettbaserte tjenester er imidlertid ikke bare knyttet opp mot betalingsoverføring. Ved siden av denne betalingsoverføringstjenesten tilbys det for eksempel flere tilleggstjenester som kunden kan inngå særskilt avtale om. Slik sett kan nettbanktjenesten anses som en overordnet «portal» som tilrettelegger for flere tilleggstjenester, eksempelvis handel med verdipapirer, betaling til utlandet mv. Noen banker har lagt dette opp slik at en nettbankavtale fungerer som en hovedavtale som åpner for å inngå underliggende avtaler om én eller flere av tjenester som tilbys over Internett. I dette ligger også at nettbanktjenesten vil variere fra bank til bank både med henblikk på struktur og vilkår for bruk.[1] Dette innebærer også variasjoner i hvilke sikkerhetsprosedyrer som må følges av kunden. Avveiningen mellom brukervennlighet og sikkerhet er slik sett forskjellig fra bank til bank og et viktig element i forhold til

[1] Som utgangspunkt ligger imidlertid standardiserte kontoavtaler som er utarbeidet av de sentrale interesseorganisasjonene Sparebankforeningen og Finansnæringens Hovedorganisasjon.

ansvarsplassering av eventuelle tap. Sider av dette temaet drøftes i avsnitt 5.3 om generelle risikoaspekter nedenfor. *Banklovkommisjonen* bemerker at spørsmål knyttet til de øvrige tjenester som følger med nettbanktjenesten ikke er tema i denne utredningen, jf. forutsetningene i mandatet. Den videre redegjørelsen er således begrenset til spørsmål knyttet til betalingsoverføring via nettbaserte betalingstjenester. Muligheten til å foreta kjøp over Internett, for eksempel ved hjelp av BankAxess er derfor et sideordnet tema. Det er kontodisponeringen som er det essensielle, selv om det er viktig å merke seg at lignende risiko- og tapssituasjoner kan oppstå i andre sammenhenger.

Det som gjelder generelt for alle slike nettbaserte tjenester, er at brukeren må legitimere seg i henhold til en nærmere bestemt sikkerhetsprosedyre. Man har her å gjøre med en form for brukerlegitimasjon i motsetning til vanlige bankkontoregler som gjelder ved overføring via eksempelvis bankgiro. Ved en slik prosedyre stilles det ikke nødvendigvis krav om underskrift eller annen form for manuell legitimasjon for de enkelte betalingsoppdragene. Tilgangen er i stedet knyttet opp mot personlige legitimasjonselementer som fødselsnummer, kontonummer, PIN-koder, passord og engangskoder. Selve informasjonen om betalingstransaksjonen overføres på et elektronisk medium som for eksempel telefonlinje, nettverkslinje eller annet lagringsmiddel, og ved selve overføringen vil for øvrig spørsmål om tid og sted for betalingen være relevante temaer. De ansvars- og risikovurderinger som *Banklovkommisjonen* gjorde i tilknytning til betalingskortene i sin Utredning nr. 1, bør imidlertid utbygges til også å omfatte ansvar og risiko rundt selve bruken av slike andre nettbaserte betalingstjenester.

Betalingsoverføring ved bruk av tradisjonell giro og betalingskort er redegjort for i henholdsvis kapittel 3 og 4 foran. Her er aktuelle risikospørsmål gjennomgått med en etterfølgende beskrivelse av den gjeldende ansvarsregulering for potensielle tapssituasjoner. *Banklovkommisjonen* har ikke sett et behov for nærmere lovregulering av slike betalingstjenester, jf. særlig avsnittene 3.5 og 4.6 foran.

Før *Banklovkommisjonen* gir en redegjørelse for risikobildet ved bruk av nettbaserte betalingstjenester, med utgangspunkt i nettbanktjenesten, og gjeldende ansvarsregulering ved eventuelle tapssituasjoner, gis det en oversikt over selve bruken av de nettbaserte betalingstjenestene og dens utvikling innenfor betalingsformidling, se avsnitt 5.2 flg. Det nevnes i denne sammenheng at visse tjenester som er tilbudt innenfor telefonbank, ikke er å anse som en betalingstjeneste. For å danne et helhetlig bilde av denne banktjenesten, er det likevel gitt en beskrivelse av samtlige tjenester på dette området. Avgrensninger mot tjenester som ikke er å anse som betalingsoverføring gjøres derfor løpende i avsnitt 5.2.2 om bruk av telefonbank.

5.2 Virkemåten

5.2.1 Bruk av nettbank

Internett ble startet rundt 1970 og Norge fikk sin første tilknytning allerede i 1973. Fra midten av 80-tallet begynte Internett å få betydning som kommunikasjonskanal for studenter og forskere i den vestlige verden. Det var imidlertid først på 1990-tallet at Internett fremsto som interessant for en bredere gruppe av befolkningen, og dermed også for kommersielle aktører. Siden 1993 har nettet vokst raskt på internasjonal basis. Tall fra 2005 viser at Norge ligger helt i europatoppen både når det gjelder handel, bruk av finansielle tjenester og tilegnelse av informasjon og nyheter på Internett. Av landets hustander i 2005 hadde 64 prosent internettilkobling, og to tredjedeler av disse er bredbånd.[2] Det er imidlertid langt flere som bruker Internett, og i alderen 15-29 år er andelen av brukere på 97 prosent.[3]

Parallelt med utbredelsen av personlige datamaskiner og internettilkobling i den private sektor, så bankene både en mulighet og et behov for å utvikle pc-baserte systemer hvor privatkunder blant annet selv kan initiere betalingsoppdrag og få tilgang til saldoinformasjon og foreta annen kommunikasjon med banken. I 1996 var dette noe som kun var i prøvefasen, og det var land som Frankrike og USA som hadde kommet lengst i denne utviklingen. I dag er nettbank eller hjemmebank, et vanlig fenomen i de norske hjem. Det er som nevnt i avsnitt 1.3 foran ca. 2,8 millioner nettbankkunder i Norge. Det er antatt at 2 millioner personer i Norge bruker nettbanktjenesten hver uke.[4] I 2007 ble det gjennomført totalt ca. 319 millioner nettbanktransaksjoner. Av disse ble ca. 154 millioner transaksjoner utført av privatpersoner. Det er videre ventet at utbredelsen av slike systemer vil øke i tiden fremover. Tilfanget av nye nettbankkunder har økt jevnlig de siste årene. I 2007 var det en økning i antall nettbankkunder på 300.000. Det å bruke nettbank er nå like vanlig som å bruke e-post og Internett for å innhente informasjon.[5]

[2] NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.2.2.
[3] Sparebankforeningens Nettbankundersøkelse 2008 side 5.
[4] Sparebankforeningens Nettbankundersøkelse 2008 side 15.
[5] Sparebankforeningens Nettbankundersøkelse 2008 side 15.

Rutinene for hvordan man blir nettbankkunde og kan bruke nettbanktjenesten, vil naturligvis variere mye fra bank til bank. *Banklovkommisjonen* har i dette henseende tatt utgangspunkt i flere av de etablerte norske og nordiske nettbankene, og forsøkt på best mulig vis å gi et enhetlig bilde av fremgangsmåten for å bli nettbankkunde.

1) *Avtale og tilgang.* For å ta i bruk nettbanktjenesten må kunden inngå avtale med banken om dette. Dette kan normalt både skje ved fremmøte i banken eller ved bruk av bankens hjemmesider. Noen banker har ikke vanlige ekspedisjonssteder, slik at eneste måten er å etablere kundeforholdet via bankens hjemmesider. Det er særlig selve bestillingen av nettbanktjenesten som er forskjellig mellom de nevnte bankinstitusjonene, selv om den videre prosessen også vil variere fra bank til bank ut fra den enkeltes vurdering av hvordan de aktuelle sikkerhetskrav bør overholdes på best mulig måte. De konkrete beskrivelsene i det følgende er derfor ikke å anse som sammenfallende for samtlige bankinstitusjoner med nettbanktjeneste.

For å etablere kundeforhold i de rene nettbaserte bankene (uten bankfilialer), må man først registrere en rekke personopplysninger på hjemmesiden til banken, blant annet fødselsnummer og øvrig kontaktinformasjon. Kunden blir gjerne bedt om å akseptere kontoavtalen inklusive vilkår for elektronisk regningsbetaling på nettet. Dette skjer ved at vedkommende huker av i en rubrikk som anses som en bekreftelse på at avtalen er lest og akseptert. Det stilles således ikke krav om underskrift for inngåelse av slike kontoavtaler, jf. for så vidt finansavtaleloven § 8 annet ledd og avsnitt 2.2 foran.

For å kunne benytte seg av nettbanktjenesten til en bank som har bankfilialer, er fremgangsmåten noe annerledes. Dersom vedkommende ikke allerede er kunde i banken, må vedkommende søke om dette, enten via bankens nettside eller ved å gå til en av bankens filialer. Ved personlig oppmøte må kunden oppgi nødvendige opplysninger og signere avtaledokumenter med kontoavtalen som hoveddokument. Nettbankavtalen kan også inngås i denne sammenheng. Det er videre mulig å bli kunde i banken ved hjelp av bankens nettside, selv om den videre prosessen avviker fra de rene nettbaserte bankene. Vedkommende må taste inn nødvendig informasjon og samtidig bestille nettbanktjenesten. Bankinstitusjonens kundesenter ringer så vedkommende opp for å få oppgitt nødvendig informasjon, for eksempel hvor avtaledokumentene skal sendes. Disse må kundene sende tilbake i underskrevet stand per post.

Deretter sender som oftest banken, enten den kun er nettbasert eller ikke, midlertidig PIN-kode og verktøy for generering av engangskoder per post i to forskjellige sendinger. Midlertidig PIN-kode sendes direkte til kundens bostedsadresse, men kan også sendes per SMS. For engangskodeverktøyet benyttes det imidlertid rekommandert brev til folkeregistrert adresse som vedkommende må hente på postkontoret. Her følges en prosedyre som er fastsatt i en avtale mellom banken og Posten, en såkalt PUM-avtale (Personlig Utlevering Mottakingsbevis). Dette innebærer at Posten har ansvar for å sørge for at vedkommende legitimerer seg og kopierer opplysninger om legitimasjon og fødselsnummer, slik at avsender får denne PUM-dokumentasjonen. Det er likevel viktig å merke seg at utsending av engangskodeverktøy blir sendt i vanlig postsending direkte til kundens bostedsadresse dersom denne er utgått (typisk ved kodekort) eller kunden har mistet det.

2) *Innlogging.* Innloggingsprosedyren i banken via dens nettbanktjeneste kan variere fra bank til bank. Dette gjelder både hvordan engangskoden genereres og rekkefølgen på inntastingen av den nødvendige innloggingsinformasjonen. I noen banker er det lagt opp til at det først inntastes fødselsnummer og personlig kode. Deretter må kunden ta i bruk utstyr for supplerende sikkerhetsprosedyre, typisk inntasting av en engangskode. Denne engangskoden kan enten leses ut fra for eksempel en kodekalkulator («digipass» eller lignende), et kodekort eller ved at engangskoden sendes til kundens oppgitte mobiltelefonnummer. De verktøyene som brukes for å generere disse kodene, varierer naturligvis noe og vil derfor ha betydning for sikkerheten knyttet til bruk av slike koder. I noen banker kreves det i tillegg at det lastes ned et sertifikat for å kunne logge seg inn i banken. Sertifikatet låses til den aktuelle datamaskinen som benyttes. Dersom vedkommende også vil bruke annen datamaskin for å få tilgang til sin nettbankkonto, må dette lastes ned på den aktuelle maskinen, for eksempel jobb-pc. Varigheten av sertifikatene varierer, men med maksimum gyldighetstid på ett år. Deretter må kunden laste ned nytt sertifikat.

Bankene tar i stadig større grad i bruk BankID som påloggingsmekanisme. BankID er en personlig og elektronisk legitimasjon for sikker identifisering og signering på nett. Den er basert på en samordnet infrastruktur som er utviklet av banknæringen, i regi av Finansnæringens Hovedorganisasjon og Sparebankforeningen. Over 1,5 millioner nettbankkunder benytter seg nå av dette elektroniske identitetssystemet. Flere av de største bankinstitusjonene går også over til BankID i løpet av høsten

2008. BankID legger dessuten til rette for å melde adresseforandring, kjøpe bil eller bolig og levere byggesøknad hos kommunen på Internett.[6] Det er spådd at flertallet av Norges 2,8 millioner nettbankkunder vil bruke BankID som sin elektroniske ID og signatur innen utgangen av 2008.[7] En elektronisk signatur med BankID vil være like bindende som en håndskrevet signatur på papir.

Kundene kan søke om BankID gjennom nettbanken eller ved personlig fremmøte på vanlig måte, det vil si inntasting av fødselsnummer, PIN-kode og engangskode. I praksis foregår dette ved at kunden aksepterer vilkårene for bruk av BankID.[8] Deretter må kunden velge et personlig passord som skal fungere som hans eller hennes BankID. Dette passordet skal som oftest bestå av tall og/eller bokstaver og erstatter den tidligere PIN-koden. Her er det som nevnt foran bankindividuelle forskjeller. Deretter foretas det en sjekk av om kundens datamaskin kan benytte BankID. Det stilles i denne sammenheng krav til både operativsystem, nettleser og java-program. Dette henger sammen med institusjonens ønske om å forsikre seg om at kundens tilgang til banken er tilstrekkelig sikker. BBS har verifisert en rekke kombinasjoner av disse uten at *Banklovkommisjonen* har funnet grunn til å gå nærmere inn på dette. Neste gang kunden logger seg inn i nettbanken ved bruk av BankID, vil det komme en sikkerhetsadvarsel fra BBS. Denne vil dukke opp hver gang med mindre kunden huker av for «Klarér alltid innhold fra Bankenes Betalingssentral AS». Ved bruk av BankID som innlogging vil kunden få opplyst om sist gang han eller hun var innlogget i banken og representerer et ytterligere kontrolltiltak i forhold til misbruksfaren for nettbanktjenesten.

3) *Bruk av nettbank.* Når kunden er logget på nettbanktjenesten, kan vedkommende i stor grad disponere og få oversikt over sin konto som tidligere ofte var betinget av personlig oppmøte i bankfilial. Det mest aktuelle er antagelig regningsbetaling. Dette er en form for girobetaling, og *Banklovkommisjonen* har derfor – for oversiktens del – funnet grunn til å videreføre skillet i kapittel 3 med giro, ferdigutfylte blanketter og belastningsgiro, se også punkt 4) nedenfor. Ved siden av regningsbetaling har kunden også mulighet til å overføre mellom egne konti (dersom kunden har opprettet flere i den aktuelle banken). I flere banker er det videre lagt opp til at kunden kan søke om lån, investere i fond eller aksjer, samt tegne ulike forsikringer. Disse tilleggstjenestene går ikke Banklovkommisjonen nærmere inn på, jf. også avsnitt 5.1 foran. Med tiden legges det opp til at kunden kan benytte BankID for elektronisk signering av avtaler inngått på nettet, for eksempel låneavtaler.

4) *Regningsbetaling.* Ved overføring til privatpersoner er det som oftest kunden selv som må skrive inn alle nødvendige opplysninger, og fyller på elektronisk vis inn en giroblankett. Dette henspeiler seg først og fremst på kreditkontonummer, beløp og betalingsdag.

Regningsopplysninger kan videre være ferdigutfylt av mottaker. Slike ferdigutfylte blanketter kan komme i papirbasert format, som beskrevet i avsnitt 3.2.2 foran. På nåværende tidspunkt er imidlertid et stort antall av disse blankettene knyttet direkte opp mot kundens nettbank. Dette er en form for elektronisk faktura eller elektronisk girordning og er benevnt som «eFaktura».[9] Denne tjenesten er således basert på at betalingsinstruksjonene gis i maskinlesbar form, enten direkte via terminal eller ved maskin- til maskinforbindelse. For å kunne benytte seg av denne tjenesten, må kunden inngå en avtale med tilbyder av slik faktura og akseptere at tilbyder eller kreditor sender fakturaer elektronisk til kundens nettbank. Det er således betalingsmottakeren eller kreditor som initierer de enkelte betalingene. Selve belastningene forutsetter imidlertid at kunden gjør noe aktivt, nemlig aksepterer at fakturaen legges i forfallsregisteret eller lignende. En eFakturaavtale knyttes til kundens fødselsnummer og ikke konto. Dette muliggjør valg av bank og konto for belastning hver gang. Tjenesten er slik sett bankuavhengig, og det er opp til kunden hvilken nettbankkonto som skal belastes for hver gang.

AvtaleGiro kan også sees på som en ferdigutfylt giroblankett som i mange tilfeller er direkte knyttet opp til nettbank. Det nærmere innholdet av slike belastningsfullmakter er behandlet separat i avsnitt 3.2.3 foran.

---

[6] Se også pressemelding fra Fornyings- og administrasjonsdepartementet av 3. april 2008 hvor det fremgår at Regjeringen har besluttet å opprette en offentlig infrastruktur – et samtrafikknav – for elektronisk ID. Beslutningen innebærer at man «i fremtiden kan benytte samme eID på flere offentlige elektroniske tjenester, at tjenestene blir flere og mer avanserte og at dagens pinkodekaos går mot slutten».

[7] Sparebankforeningens Nettbankundersøkelse 2008 og artikkel fra BankID.no.

[8] Søknaden legger også til rette for å kunne bestille BankAxess, som gir kunden mulighet til å betale direkte fra kontoen når han eller hun handler på nettet. Dette går ikke Banklovkommisjonen nærmere inn på.

[9] Ved utgangen av 2007 var det inngått ca. 3 millioner avtaler om slik elektronisk faktura. Det er en økning på ca. 1 million eFaktura-avtaler siden 2006.

5.2.2 Bruk av telefonbank

Kommunikasjon med bankforbindelse via telefon, kan enten gjøres ved personlig samtale mellom kunden og bankansatt eller ved at kunden taster inn nødvendige innloggingsopplysninger på telefonen (automatisk telefonbank) og deretter velger tjenester som er tilrettelagt ved hjelp av telefonens talltastatur.

1) Personlig betjening eller kundeservice gir kunden mulighet til å melde fra om mistet eller stjålet betalingskort, saldoinformasjon eller overføring mellom egne konti. Informasjon om saldo og overføring mellom egne konti krever at kunden identifiserer seg med person- eller kontonummer og oppgir et selvvalgt passord. Ettersom det ikke er mulig å foreta betalingsoverføring ved slik personlig betjening, er ikke dette å anse som en betalingstjeneste og er unntatt fra Banklovkommisjonens forslag om nytt regelverk for nettbasert betalingsoverføring.

2) Automatisk telefonbank er en banktjeneste som legger til rette for mange av de samme banktjenestene. Fra midten av 1990-tallet ble slike telefonbanker imidlertid videreutviklet til også å omfatte initiering av betalingsoppdrag. Under den automatiske telefonbanktjenesten ligger det således flere verktøy tilgjengelig for kunden, det være seg å få lest opp kontoutskrift *(kontofon)* eller foreta betalingsoverføringer *(telegiro)*. For å kunne benytte seg av en automatisk telefonbank, må kunden først aktivere tjenesten og få tilsendt en tilgangskode fra banken (vanligvis tre sifre). Det er ved beskrivelsen av disse tjenestene tatt utgangspunkt i flere norske og nordiske banker, og på best mulig vis gitt en samlet fremstilling av de ulike tjenestene.

Med *kontofon* kan kunden kun undersøke saldo og overføre penger mellom egne konti. På samme vis som ved personlig betjening, er dermed ikke dette å anse som en betalingstjeneste og er unntatt i den videre utredningen. En annen lignende tjeneste som for så vidt er knyttet opp til mobiltelefoner er såkalt *sms-bank*. Denne tjenesten er på nåværende tidspunkt ikke tilbudt av samtlige bankinstitusjoner som opererer i Norge. Innholdet i denne tjenesten varierer også. Noen banker har en ordning hvor kunden via sms kan bli varslet hver gang det innbetales lønn eller hver gang saldoen er over eller under et visst beløp. Andre banker har en ordning hvor det også kan overføres penger mellom egne konti. Ved bruk av sms-bank må kunden også få tilsendt en tilgangskode. På samme vis som ved kontofon, utelates imidlertid denne banktjenesten i den videre utredning.

Med *telegiro* kan kunden utføre enkle tjenester som regningsbetaling, administrere AvtaleGiro og få tilgang til forfallsregisteret for regningene. Dette er slik sett en betalingstjeneste som er omfattet av Banklovkommisjonens videre utredning om risiko og ansvarsregulering ved bruk av nettbasert betalingsoverføring. Telegiro kan benyttes av kundene fra deres mobiltelefon eller vanlig hustelefon. I løpet av 2007 ble det foretatt ca. 14 millioner transaksjoner ved hjelp av telegiro.[10]

3) *Mobilbank* er en forholdsvis ny form for betalingstjeneste. Det må imidlertid antas at dette er en tjeneste som vil tas i bruk i stort omfang i tiden som kommer, særlig som følge av at mobiltelefon nærmest er allemannseie.[11] Betalingsoverføring via mobilbank, forutsetter imidlertid at kunden har en mobiltelefon med nettleser. Mange av mobiltelefonene som er – og kommer – på markedet vil normalt sett ha en internettoppkoblingsfunksjon. Den fungerer slik sett som en liten bærbar datamaskin, hvor mobiltelefondisplayet erstatter dataskjermen. Bruk av mobilbank forutsetter derfor at kunden har opprettet en nettbankkonto og kan sies å være en forenklet versjon av nettbanktjenesten.

For noen mobilbanker er det imidlertid bare mulig å overføre penger mellom egne konti og få kontoopplysninger. I slike mobilbanker, er ikke sikkerhetsrutinene like strenge som ved de mer avanserte mobilbanktjenestene, og det kreves ofte bare at kunden taster inn sitt kontonummer og servicekode for å få tilgang til sin bankkonto, sml. forholdet ved personlig betjening som beskrevet foran.

Ved bruk av mobilbank hvor kunden kan betale regninger, overføre mellom egne konti, få tilgang til eFaktura, sjekke forfallsregisteret mv., er imidlertid sikkerhetsrutinene strengere. Som ved nettbank, må kunden gå frem på samme måte og taste inn brukerID (for eksempel kontonummer eller fødselsnummer), passord og engangskode. Det er videre lagt opp til at BankID kan benyttes fra en mobiltelefon.

4) Det er ellers antatt at mobiltelefoner også vil bli brukt til småbetalinger i fremtiden. Både VISA og MasterCard har utviklet et system for kontaktløse betalinger. *Banklovkommisjonen* nevner at dette er en tjeneste som ikke er direkte knyttet opp mot kundens konto og må således holdes atskilt fra utredningens hovedtema.[12] Den omfattes videre av e-pengeforetaksloven av 13. desember 2002 nr. 74

[10] Norges Banks årsrapport om betalingssystem for 2007 side 46.

[11] I 2006 hadde 93 prosent av husholdningene mobiltelefon i Norge, jf. NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.2.3.

og ikke av finansavtalelovens bestemmelser. For oversiktens skyld er det imidlertid hensiktsmessig å gi en kort beskrivelse av denne tjenesten. Tjenesten fungerer slik at en brikke blir plassert i et betalingskort eller i en mobiltelefon. Kunden betaler ved at brikken kommuniserer med en betalingsterminal når den holdes nær nok uten at det stilles krav om inntasting av personlig kode.[13] I Norges Banks årsrapport om betalingssystem for 2007 er det antatt at sikkerheten rundt slike betalingssystemer er en utfordring for bankene.[14]

5.3 Generelle risikoaspekter

Betalingsoverføring representerer en grunnleggende funksjon i all økonomisk aktivitet. Sikker og lett tilgang til effektive betalingssystemer er nødvendige forutsetninger for den enkelte brukers økonomiske aktivitet, og av avgjørende betydning for at et moderne samfunn skal fungere. Selv om institusjonene har felles beredskapsplaner, sikkerhetsstandarder og kontrollrutiner, og disse er gjenstand for kontinuerlig evaluering og ajourføring, vil det i ethvert betalingssystem eksistere risikoelementer i form av interne og eksterne feil og angrep.

Selv om nettbankene utvikler nye og mer velutrustede innloggingssystemer, som for eksempel BankID til nettbank, antar *Banklovkommisjonen* at det vanskelig vil være mulig å helgardere seg mot slike angrep.[15] Et annet forhold er at systemene kan bli sårbare dersom de i stor grad blir avhengig av en tjeneste som BankID. Dersom driftsmessige problemer skulle sette BankID ut av drift og brukeren ikke får tilgang til sin bankkonto, vil dette få konsekvenser for et stort antall brukere og samfunnet for øvrig.[16] Det samme vil for så vidt gjelde dersom oppkoblingen mot Internett brytes som følge av forhold utenfor kundens kontroll.

I avsnitt 5.2 foran er det gitt en overordnet beskrivelse av virkemåten til de ulike former for nettbasert overføring, med unntak av betalingskort. Overføring av penger ved bruk av et nettbasert betalingsoverføringssystem kan sies å representere et brukervennlig system: Kunden er ikke avhengig av å besøke en bankfilial og kan foreta overføringer fra hjemmet, jobben, under ferieopphold mv. Et nettbasert betalingsoverføringssystem kan imidlertid også sies å representere et komplisert og risikofylt kundesystem. Det henspeiler seg særlig på kundens feilbruk og andres misbruk av kundens bankkonto. Slike betalingsoverføringssystem legger i stor grad opp til en høyere grad av selvstendig brukeradferd enn andre betalingstjenester, som i sin tur kan legge til rette for flere feilbruks- og misbrukstilfeller.

Graden av risiko ved bruk av nettbasert betalingsoverføring henger slik sett i stor grad sammen med avveiningen mellom ønske om å gjøre produktet så brukervennlig som mulig og nødvendige sikkerhetsmekanismer for å hindre feil og misbruk. Som nevnt i avsnitt 1.3, er det imidlertid aldri brukervennlig å oppgi nødvendige sikkerhetsmekanismer for å hindre feil og misbruk. Visse sikkerhetstiltak må ligge i bunn. For «stor» brukervennlighet vil kunne øke sannsynligheten for flere feiltransaksjoner. For eksempel kan det nevnes at mange nettbanktjenester er lagt opp slik at kreditkontonummer og betalingsmottakers navn på tidligere transaksjoner lagres i nettbankens mottakerregister. Dersom kunden skal utføre flere overføringer til denne mottakeren, kan han eller hun enkelt søke etter vedkommende i et register som kun er tilgjengelig for kunden. Det kan her tenkes at kunden ved første overføring tastet inn feil (men likevel gyldig) kontonummer uten at dette ble oppdaget, slik at flere overføringer går til feil person. Ordningen med mottakerregisteret er svært brukervennlig, men dersom det ikke oppdateres jevnlig av kunden med nye, korrekte mottakeropplysninger vil bruken kunne medføre feiltransaksjoner. Det kan videre tenkes at betalingsopplysningene er riktige, men foreldet i den forstand at mottaker har endret kontonummer. Det følger for så vidt av tiltak nr. 13 fra banknæringen selv at bankene bør legge til rette for at kunden kan gjennomføre periodisk oppdatering av mottakerregisteret. Dette er så langt Banklovkommisjonen er kjent med gjennomført for alle nettbanktjenestene. Det at det ble inntatt som et tiltak, viser at det er et aktuelt problem også sett fra næringens side. Det vises for øvrig til avsnitt 1.3 foran. Slike potensielle feiloverføringstilfeller er imidlertid ikke like aktuelt for de tilfeller hvor mottakeren har endret sitt kontonummer, ettersom det vil skje en omadressering hos BBS, slik at beløpet overføres til det nye kontonummeret i stedet.

---

[12] Den er for øvrig kontobasert via en mellomavregningssentral uten at *Banklovkommisjonen* finner grunn til å gå nærmere inn på dette.

[13] Det samme vil kunne tenkes å gjelde for klokker, forskjellige slags personlige kort mv. Dette systemet gjelder for eksempel for kortbrikkene ved innkjøring gjennom bomstasjoner på veiene.

[14] Årsrapporten 2007 side 10.

[15] I denne sammenheng nevnes at en forskergruppe ved Universitet i Bergen nylig klarte å bryte seg inn i to nettbanker som bruker BankID som elektronisk signatur og identifikasjon, se Aftenposten side 7, tirsdag 26. februar 2008.

[16] Norges Banks årsrapport om betalingssystem 2007 side 10.

Temaet risiko ved bruk av nettbasert betalingsoverføring, henspeiler seg i hovedsak på de potensielle tapssituasjoner som kan forekomme ved kundens bruk av sin bankkonto(i) gjennom oppkobling til Internett eller telefonnettverk. Det er flere omstendigheter som kan føre til tap, og det er viktig å merke seg at disse omstendighetene er av dynamisk karakter. Selv om bankene iverksetter tiltak med flere sikkerhetsrutiner og kontrollordninger, vil det som nevnt være vanskelig å totalsikre seg mot alle risikoelementer som er tilknyttet slikt kontohold. Det er særlig kundens egne feil og tredjemanns misbruk som er fremtredende i denne sammenhengen. Svikt i systemet er en potensiell feilkilde, men ikke forutsatt utredet i denne omgang.[17]

Feilbruk og misbruk representerer aktuelle tapssituasjoner, men er ikke nødvendigvis selvstendige og separate risikoforhold. De må i flere tilfeller sees i sammenheng, jf. særlig avsnitt 6.1.3 nedenfor. Det er gitt en redegjørelse for risikoen for kundens egne feil i avsnitt 5.4 nedenfor. Risikoen for tredjemanns misbruk er det redegjort for i avsnitt 5.6. Redegjørelsen er først og fremst knyttet opp til bruk av nettbank. Risikoelementene ved slik bruk vil i stor grad være tilsvarende for bruk av telefonbank. *Banklovkommisjonen* har likevel funnet det hensiktsmessig å si noe særskilt om telefonbank avslutningsvis i avsnittet om risikoaspekter, både i forhold til egne feil og andres misbruk, se henholdsvis avsnitt 5.4.2 og 5.6.2.

Det nevnes også at de risikoelementer som skal gjennomgås, vil kunne være relevant i forhold til en vurdering av ansvarsplassering av det økonomiske tapet som kan oppstå. Her kan det tenkes flere forhold som må tas i betraktning, blant annet nivået av sikkerhet i nettbanksystemet for at feil fra kunden kan oppdages og kundens egen aktpågivenhet. Brukeratferd må sees i sammenheng med tapssituasjoner som kan oppstå som følge av enten feilbruk eller misbruk, og er således et viktig element i drøftelsen av hvordan ansvarsplasseringen bør fremstå. Det vises særlig til avsnitt 6.3 flg. nedenfor om hovedprinsippene i *Banklovkommisjonens* lovforslag.

5.4 Risiko for kundens egne feil

5.4.1 Nettbank

Tap som er forårsaket av forhold på kundens side, kan ha sitt utspring i forskjellige forhold. De tradisjonelle typetilfellene er feiltastingstilfellene, det vil si inntasting av feil kontonummer og/eller feil beløp, hvor kunden ikke oppdager feilen før betalingsoppdraget utføres. Ved siden av feil knyttet opp til kontonummer, kan det dessuten kunne tenkes andre inntastingsfeil som kan lede til økonomisk tap for kunden. For eksempel at kunden taster feil dato for belastning av oppdraget, slik at kreditor ikke mottar betalingen innen en eventuell betalingsfrist og ilegger kunden et purregebyr og/eller inkassogebyr. Utover disse typetilfellene er det andre avvik og feil fra kundens side som kan forekomme. Disse må imidlertid sees i sammenheng med potensielt misbruk fra tredjemenn, for eksempel ved at kunden har oppbevart nødvendig brukerlegitimasjon på feil måte, og er i stedet inntatt i avsnitt 5.6 om risikoen for andres misbruk.

Utilsiktede betalingsoverføringer er først og fremst aktuelt i forhold til vanlig girobetaling. Med eFaktura er ikke dette en like nærliggende risikofaktor, ettersom kunden legger til grunn at betalingsmottakeren har sendt over riktig betalingsinformasjon og iverksetter betalingen ved å akseptere denne i nettbanken. Som nevnt i avsnitt 3.3.1, jf. også avsnitt 3.5 foran, vurderte *Banklovkommisjonen* det slik at det vanskelig kunne tenkes å oppstå tapssituasjoner for kunden som følge av feilbruk. Grunnlaget for denne vurderingen må anses å være forsterket i forhold til elektronisk faktura hvor handlingsrommet for å kunne gjøre feil er enda mindre. Banklovkommisjonen antar at risikobildet for belastningsgiro er forholdsvis likt og at tapssituasjoner også sjelden vil oppstå her. I det følgende er det dermed risikobildet for de tradisjonelle girooverføringene som vurderes nærmere. Det er i disse situasjonene at feilaktig utførte betalingsoverføringer er en nærliggende risikofaktor.

Avvik i form av feil bruk av tjenesten kan medføre fare for store økonomiske tap, og har et høyere risikoinnhold enn ved eksempelvis betalingskort. Selv om det for de store betalingsoverføringene kan være særskilte sikkerhetsrutiner som må følges, er beløpsrammene for betalingsoverføringer som oftest større for nettbank enn for betalingskort.[18] I praksis har dette også vist seg å være en reell risikofaktor. I Bankklagenemndas saker BKN-07015 og BKN-07016 hadde en kunde tastet feil ved overføring av 500.000 kroner, og nemnda kom til at pengene ikke kunne kreves erstattet av banken. Etter at banknæringen innførte nye kontrollrutiner, se punkt 1.3 foran, er det imidlertid forholdsvis usannsynlig at lignende tilfeller vil opp-

[17] Det vises for så vidt til det utredningsarbeidet arbeidsgruppen for gjennomføring av betalingstjenestedirektivet er forutsatt å nedlegge, jf. avsnitt 1.2 foran.

[18] Det vises for øvrig til avsnitt 6.2.3 nedenfor om beløpsgrenser ved bruk av nettbanktjenesten.

stå igjen, da det her – fra bankens side – var hevdet at kunden hadde tastet et nummer for mye som ikke var blitt oppdaget av nettbanksystemet. Denne saken er nå for så vidt forlikt mellom partene, og kunden fikk tilbakeført det omtvistede beløpet. Banken erkjente imidlertid ikke ansvar og forliket har slik sett begrenset rettskildemessig verdi.

Tastefeil som overses av kunden i den videre behandlingen av betalingsoppdraget vil med sikkerhet alltid kunne forekomme på grunn av det meget store antallet nettbanktransaksjoner.[19] Et annet spørsmål er hvorvidt risikoen for slike feil manifesterer seg i et økonomisk tap for kunden. For det første skal det visstnok være svært vanskelig å «treffe» et reelt kontonummer ved feiltasting.

For det andre er det hovedsakelig overføringer til privatpersoner eller mindre foretak som kan lede til slike tap. Ved regningsbetaling til større foretak stiller som oftest kreditor krav om at kunden også taster inn et KID-nummer. Dette nummeret er knyttet opp mot kundens gjeldsforhold til foretaket. Det er imidlertid ikke en forutsetning at kunden taster inn riktig kontonummer. Slik sett kan det forekomme feiloverføringer i disse tilfellene. Likevel er ikke risikoen for at slike transaksjoner medfører tap for kunden særlig stor, ca. 10 prosent sannsynlighet er prognosen fra næringen. For at en betalingsoverføring med påført KID-nummer skal kunne gå igjennom, er det en forutsetning at oppført mottaker kan motta transaksjoner med KID-nummer. Dette vil si at alle privatpersoner er unntatt, samt visse foretak.[20] Kunden vil i disse tilfellene få en feilmelding og transaksjonen gjennomføres ikke. Dersom kunden skulle taste kontonummer til en mottaker som kan motta KID-transaksjoner, må det dessuten legges til grunn at det ikke vil være vanskelig å kreve pengene tilbake igjen. Her må det for øvrig gjøres unntak mot kredittkortselskapene hvor feilaktig innbetaling kan godskrives en kredittkortkundes saldo. Det må uansett kunne legges til grunn at det kun er et begrenset antall overføringer som kan lede til økonomisk tap dersom kunden gjør en feil ved inntasting av betalingsinformasjon. Utslaget for den enkelte kan imidlertid være meget alvorlig dersom det først gjøres en feil som ikke blir oppdaget før betalingsoppdraget iverksettes.

For det tredje vil slike saker bare komme på spissen så sant innehaver av kontoen som pengene kommer inn på faktisk bruker pengene og ikke vil eller kan tilbakebetale beløpet. Dette vil som oftest være tilfelle dersom det dreier seg om privatpersoner. I tilfeller ved feiloverføringer til større foretak vil nok tilbakebetaling kunne skje i langt større grad.

For det fjerde vil kunden og bankinstitusjonen kunne komme til enighet angående det aktuelle tapet. Det nevnes i denne sammenheng at saken vedrørende overføring av 500.000 kroner ble forlikt mellom partene.

Det bør for øvrig også her nevnes at kunden feilaktig kan bli tilsendt en regning flere ganger, enten i papirformat eller som eFaktura. Selv om dette normalt sett vil bli rettet opp i, enten av Posten eller kreditor, er det en risiko for at kunden ikke får pengene tilbakebetalt.

Feiloverføringer er dessuten forsøkt eliminert gjennom flere tiltak. Banknæringen nedsatte, som nevnt i avsnitt 1.3 foran, en arbeidsgruppe som skulle se på tiltak for å øke tryggheten for at brukeren ikke utfører utilsiktede betalingsoverføringer. For å øke kundenes trygghet, ble det blant annet stilt krav om at det skulle gis feilmelding dersom det ble tastet inn for mange sifre, klart skille mellom kroner og øre, krav om at kunden aktivt tar stilling til informasjonen i kontrollbildet før vedkommende kan gå videre og betalingen blir iverksatt. Videre ble det foreslått at nettbankene som standard har en beløpsgrense per transaksjon og/eller for transaksjonsbeløp innen en periode. Dette er på nåværende tidspunkt gjennomført for samtlige nettbanktjenester.

De nevnte sikringstiltakene må også sees i sammenheng med avsnitt 5.6 nedenfor om misbruk fra tredjemann. Tiltakene som er foreslått, tilrettelegger for en prosess som krever mer bevisst brukerinteraksjon og som gjør det vanskeligere for svindlere å overta. Her kommer for øvrig avveiningen sikkerhet versus brukervennlighet inn. Dette temaet har imidlertid ikke Banklovkommisjonen funnet hensiktsmessig å drøfte nærmere i denne utredningen, men sikkerhetsprosedyrer er vektlagt i den nærmere utformingen av regelverket, jf. særlig avsnitt 6.3.2 nedenfor om vurderingen av om kunden har opptrådt grovt uaktsomt eller ikke.

Det bør også nevnes at det er tenkelig at bankenes nettbanktjenester vil kunne utbygges for å gjøre det sikrere for kunden. *Banklovkommisjonen* har funnet grunn til å nevne at et kontrollsystem

[19] Banklovkommisjonen er kjent med en rapport av professor Kai A. Olsen fra Høgskolen i Molde med tittel «Inntasting i nettbank». Denne rapporten viser at feiltasting er en faktisk risikofaktor ved regningsbetaling i nettbank.

[20] For å kunne anvende KID i betalingsoverføringen, må betalingsmottaker ha inngått en såkalt OCR-avtale med banken sin. Om mottaker er liten eller stor er i denne sammenheng ikke alltid relevant. For eksempel vil en idrettsforening med mange medlemmer kunne ha behov for en OCR-konto for å skille innbetalte medlemskontingenter og treningsavgifter fra hverandre ved bruk av ordningen med KID.

hvor navn sjekkes opp mot kontonummer kan være aktuelt, jf. for så vidt noe av den diskusjonen som var oppe i forbindelse med forslaget om såkalt kontonummerportabilitet, uten at *Banklovkommisjonen* finner grunn til å gå nærmere inn på dette. Et slikt system vil kunne redusere risikoen for utilsiktede transaksjoner. Ordningen kunne vært lagt opp på den måten at betalingsmottakers bankinstitusjon kryssjekker navn og kontonummer. Det nevnes i denne sammenheng at bankene gir mottaker av pengene beskjed om hvem de kom fra, jf. for så vidt finansavtaleloven § 30 tredje ledd annet punktum og avsnitt 2.3.1 foran. Slik sett må det legges til grunn at bankene har en viss kommunikasjon seg imellom, og at dette eventuelt kunne utbygges til en kontroll av det nærmere innhold av betalingsoverføringen. Dette vil imidlertid kunne skape problemer i forhold til eventuelle betalingsfrister, men også i forhold til taushetsregler og personvern uten at *Banklovkommisjonen* finner grunn til å gå nærmere inn på dette. Dersom kunden for eksempel har tastet riktig kontonummer, men *uriktig navn,* vil ikke den tilsiktede transaksjonen bli oppfylt innen fastsatt frist. En slik ordning vil også kunne reise særskilte problemer og avgrensningsspørsmål bankene imellom. Det nevnes også at risikoen for at det gjøres feiloverføringer bare reduseres i en slik ordning. Risikoen for at kunden likevel går frem på en måte som medfører at det foretas en feil betalingsoverføring, vil alltid kunne ligge der, så lenge det er kunden selv som iverksetter betalingsoverføringen.

Uavhengig av de tiltakene som er iverksatt av næringen eller som kan tenkes iverksatt, er *Banklovkommisjonen* derfor av den oppfatning at det uansett foreligger en reell mulighet for tapssituasjoner som er foranlediget av forhold på kundens side, noe som i sin tur kan utgjøre store utslag på dennes økonomi. Betalingsoverføringer som gjennomføres av kunden selv gjennom nettbaserte betalingstjenester, innebærer at kunden må forholde seg til flere viktige elementer på egenhånd uten hjelp fra bankfunksjonærer eller lignende. I denne forbindelse vil det med sikkerhet oppstå et stort antall feil fra kundens side, som for eksempel inntasting av feil kontonummer eller beløp uten at dette oppdages før betalingsoppdraget iverksettes. Ved slike feil, kan det ikke utelukkes at kunden faktisk treffer et gyldig kontonummer, at mottaker urettmessig bruker pengene og at institusjonen ikke er villig til å inngå et forlik om den omtvistede disposisjonen. Etter *Banklovkommisjonens* mening må det være tilstrekkelig at det faktisk foreligger en risiko for tap ved egne feil, om enn liten ut fra dagens sikringstiltak, til at man vurderer tiltak som tar sikte på å redusere konsekvensene for den enkelte av slike tap. Den videre behovsvurderingen av om det bør innføres et særskilt regelsett for de nettbaserte betalingstjenestene, er gitt i avsnitt 6.1.3 nedenfor.

5.4.2 Telefonbank

I forhold til telefonbank og oppståtte tapssituasjoner som er foranlediget av forhold på kundens side, er det ikke like nødvendig å skille mellom telegiro og mobilbank. Det er særlig feiloverføringer som er aktuelle i denne sammenheng, og det vil i stor grad bero på kundens håndtering av telefonen, enten det dreier seg om en mobiltelefon eller vanlig hustelefon. Det bør for øvrig sies at hustelefon og mobiltelefon har langt mindre taster enn datamaskiner. Muligheten for å taste feil er slik sett større for disse telefonapparatene.

Ved overføringer ved hjelp av telegiro (enten ved bruk av mobiltelefon eller hustelefon), er betalingsoppdrag imidlertid gjenstand for en bekreftelse på auditiv opplesning av hva kunden har tastet. Ved mobilbank er det en visuell bekreftelse som må gjøres. Det legges til grunn at det er enklere for kunden å forsikre seg om at det er inntastet riktig informasjon som følge av auditiv bekreftelse over telefon enn visuell bekreftelse på et forholdsvis lite skjermbilde. Slik sett er det nærliggende å anta at det er en større risiko for feiloverføringer ved bruk av mobilbank, særlig som følge av sammenhengen mellom inntasting via små taster og visuell bekreftelse på et forholdsvis lite format. Når det gjelder sikkerheten i forbindelse med selve innloggingen på mobilbank, nevnes det for øvrig at denne er bedret som følge av innføringen av BankID, jf. avsnitt 5.2.2 foran.

5.5 Ansvarsregulering ved kundens egne feil

5.5.1 Innledning

Drøftelsen i avsnitt 5.4 foran, viser at det eksisterer risikofaktorer av varierende karakter og omfang ved bruk av nettbaserte betalingstjenester. Slike risikofaktorer kan imidlertid til dels bøtes på ved nærmere bestemte ansvarsregler mellom kunde og institusjon som regulerer de tapssituasjoner som måtte oppstå ved bruk av slike overføringsmekanismer. I det følgende redegjøres det for nåværende ansvarsregulering mellom kunde og institusjon dersom det skulle oppstå tap som er foranlediget av kundens feilbruk av en nettbasert betalingsbeta-

lingstjeneste. Det er tatt utgangspunkt i *kontoavtalen* mellom kunden og institusjonen, se avsnitt 5.5.2 nedenfor.

Når det gjelder aktuell *lovgivning* i forhold til en ansvarsregulering mellom kunde og institusjon ved bruk av nettbaserte betalingstjenester, må det først og fremst sees hen til finansavtaleloven. Aktuelle bestemmelser i denne loven er gjennomgått i kapittel 2 foran, slik at drøftelsen i avsnitt 5.5.3 nedenfor i stor grad er knyttet opp mot dette kapitlet. Visse bestemmelser i ehandelsloven og betalingssystemloven er imidlertid også av interesse, se avsnitt 5.5.4 og 5.5.5. I avsnitt 5.7 og 5.8 er andre aktuelle rettsregler og rettsprinsipper gjennomgått.

5.5.2 Kontoavtalen

Kontoavtalen mellom kunden og institusjonen er i stor grad et kompromiss mellom representanter for institusjonene på den ene siden og representanter for forbrukerne på den andre siden. Etter at Banklovkommisjonen avga sin Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) som ledet til finansavtaleloven, er det imidlertid fastsatt en rekke lovmessige minimumskrav som er inntatt i de nåværende kontoavtalene. Disponering av nettbankkonto er ofte undergitt særlige avtalevilkår som er underordnet hoveddokumentet om kontohold. Benevnelsen «kontoavtalen» skal i det følgende anses å omfatte alle avtalevilkår som har betydning for bruk av nettbanktjenesten, enten de fremgår av de særlige eller av de generelle vilkårene.

Banklovkommisjonens gjennomgang av flere kontoavtaler, etterlater det inntrykk at avtalene ikke går noe lenger enn de lovfastsatte kravene, selv om avtalenes ordlyd kan være mer konkret enn lovbestemmelsene. Det nevnes at kontoavtalene om nettbetaling omfatter betalingstjenester ved bruk av et elektronisk kontaktpunkt. Slik sett er både nettbank- og telefonbanktjenesten omfattet av avtalene, noe som for så vidt er eksplisitt fastslått i flere av kontoavtalene.

Kontoavtalen inneholder først og fremst regler om kontoopprettelse, kontoinformasjon og kontroll. Det er videre gitt særlige regler om girooverføringer og betaling til og fra utlandet. Feilaktig godskrivning og belastning, samt regler om ansvar ved andres misbruk er også regulert i avtalen.

Ansvarsforholdet mellom kunde og institusjon ved oppstått tap som følge av kundens feilbruk, er imidlertid kun regulert i begrenset omfang i kontoavtalene. For de regulære girooverføringer som utføres ved hjelp av nettbaserte betalingstjenester, er det i flere av kontoavtalene for det første bestemt at beløpet overføres til oppgitt kontonummer. For det andre er det bestemt at dette også gjelder i de tilfeller oppgitt kontonummer tilhører en annen enn den mottaker som er oppgitt med navn og adresse på den nettbaserte giroblanketten. Dette er formulert som at kunden har ansvar for tap som skyldes feil registrering.

I noen kontoavtaler er det videre bestemt at institusjonen ikke er ansvarlig for tap som skyldes «ukorrekt bruk» av kunden. Som eksempel er nevnt fullmaktsoverskridelser, men det er nærliggende å anta at «ukorrekt bruk» også vil omfatte annen feilbruk av kunden. Dette må antas å kunne omfatte feiltasting av beløp eller kontonummer, uten at kunden oppdager dette før betalingsoppdraget iverksettes. Dette dekkes for så vidt av reglene angående girooverføringer som nevnt i avsnittet foran. Slike bestemmelser må videre antas å ha en side mot misbruk fra andre, og er således utdypet nærmere i avsnitt 5.7 nedenfor under temaet ansvarsregulering ved andres misbruk.

Dersom det oppstår en feil som kunden selv oppdager, er det imidlertid interessant å se på kundens mulighet til å tilbakekalle betalingsoppdraget. Kunden vil da kunne forhindre at beløpet overføres til en uvedkommende som ikke vil, eller kan, tilbakebetale beløpet. Dette er regulert både i de generelle vilkårene og de særlige vilkår som gjelder for nettbanktjenesten.

De generelle vilkårene må antas å gjelde så langt de er anvendelige for betalingsoppdrag utført gjennom nettbanktjenesten. Her er det bestemt at banken skal medvirke til kundens ønske om å tilbakekalle oppdraget, jf. for så vidt finansavtaleloven § 28 og avsnitt 2.5 foran. Det er imidlertid bestemt at betalingsoppdraget ikke kan tilbakekalles etter at det er sendt til bankenes avregningssentral for avregning bankene imellom. Betalingsoppdraget kan heller ikke tilbakekalles dersom banken etter en anmodning fra kontohaver har, eller kan anses å ha, bekreftet overfor mottaker at betalingen vil bli gjennomført.

Disse reglene må imidlertid sees i sammenheng med de særlige reglene som gjelder for bruk av nettbanktjenesten. I forhold til tilbakekall av betalingsoppdrag, er det her bestemt at dersom kontohaver ikke ønsker at banken skal gjennomføre et betalingsoppdrag, kan kontohaver til og med dagen før avtalt betalingsdag, stanse oppdraget ved bruk av funksjoner i nettbanktjenesten eller ved henvendelse til banken. Det er således ikke knyttet opp mot tidspunktet avregningssentralen mottar betalingsoppdraget. Imidlertid vil

avtalt betalingsdag normalt være den dagen beløpet blir avregnet og godskrevet i mottakerens bank. Dette følger av nettbankavtalens standardvilkår om bankers behandling av oppdraget og må således anses å være i overensstemmelse med finansavtalelovens regler om frist for tilbakekall, jf. finansavtaleloven §§ 28 og 39, sml. også avtaleloven § 7 om tilbakekall av tilbud.

Dersom betalingsdagen ikke er en virkedag, skjer imidlertid belastningen førstkommende virkedag. Det bør uansett legges til grunn at kunden må melde fra om tilbakekallingen dagen før avtalt betalingsdag, selv om dette ikke er en virkedag.

5.5.3 Bestemmelser i finansavtaleloven

Finansavtaleloven § 1 gjelder for avtaler og oppdrag om finansielle tjenester med finansinstitusjoner. Slike institusjoner er nærmere definert i finansieringsvirksomhetsloven av 10. juni 1988 nr. 40 §§ 1-2 og 1-3 og omfatter blant annet banker. På nåværende tidspunkt er det kun etablerte banker som tilbyr betalingstjenester gjennom nettbaserte kommunikasjonspunkter, som Internett og telefoni. Med implementering av betalingstjenestedirektivet, er det imidlertid lagt opp til at andre foretak kan tilby slike tjenester, typisk finansieringsforetak.

I kapittel 2 er det foretatt en gjennomgang av flere bestemmelser i finansavtaleloven. I dette avsnittet gis det en oppsummering av denne gjennomgangen så langt den kan antas å ha betydning i forhold til spørsmålet om ansvarsplassering ved tap oppstått som følge av kundens egne feil i sin bruk av tjenesten. Etter finansavtaleloven § 24 første ledd er det bestemt at kontohaveren kan bruke kontoen til innskudd, uttak og betalingsoverføringer i samsvar med kontoavtalen, se også avsnitt 2.3.1 foran. En gjennomgang av kontoavtalens regler er gjennomgått i avsnitt 5.5.2 foran.

Når det gjelder tid og sted for betaling og kundens mulighet til å tilbakekalle et oppdrag dersom denne oppdager at det har skjedd en feil ved betalingsoverføringen, typisk feil mottaker eller beløp, er disse reglene nedfelt i finansavtaleloven §§ 28 og 39. Reglene er redegjort for i avsnittene 2.3.2 og 2.5 foran. Videre er det i avsnitt 5.5.2 foran redegjort for hvorledes dette er regulert etter kontoavtalens regler. Der ble det konkludert med at kunden ikke har mulighet til å tilbakekalle betalingsoppdraget så lenge dette har nådd avregningssentralen. Etter finansavtaleloven § 39 er imidlertid utgangspunktet at beløpet er godskrevet mottakerens institusjon. I nettbanksammenheng vil dette, som nevnt i avsnitt 5.5.2 foran, bety at betalingsoppdraget er sendt fra kundens bankinstitusjon til avregningssentralen for avregning av beløpet til mottakerens institusjon.

Finansavtalelovens regler om feilbelastninger av konto er heller ikke aktuell i forhold til feilbruk av kunden. Som nevnt i avsnitt 2.4. foran, gjelder denne bestemmelsen i de tilfeller hvor det er en feil fra institusjonen selv som har forårsaket belastningen. Dersom det er kunden selv som har tastet feil kontonummer eller beløp og ikke oppdaget dette før oppdraget er iverksatt, er ikke denne bestemmelsen anvendelig.

Videre har *Banklovkommisjonen* funnet grunn til å nevne finansavtalelovens regler om lemping, jf. lovens § 36. Her er det bestemt at kontohavers ansvar kan lempes med hensyn til blant annet manglende aktsomhet eller andre forhold på institusjonens side. Videre dersom betalingssystemet ikke oppfyller forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner. En feil fra kundens side kan i visse situasjoner hevdes å burde bli oppdaget av bankens sikkerhetsordninger. Bestemmelsen gjelder imidlertid kun for andres misbruk, og eventuell lemping av ansvar må knyttes opp til slike misbrukssituasjoner. Spørsmålet om tilfredsstillende sikkerhetsrutiner og ansvar for dette, drøftes for så vidt, i tråd med mandatets forutsetninger, i avsnitt 6.2.2 nedenfor.

Banklovkommisjonen har ellers ikke funnet grunn til å gå nærmere inn på de øvrige reglene i finansavtaleloven i dette avsnittet, men viser i stedet til gjennomgangen av aktuelle bestemmelser i loven i kapittel 2 foran.

5.5.4 Bestemmelser i ehandelsloven

Andre lovbestemmelser av betydning i forholdet mellom kunde og institusjon ved bruk av nettbaserte betalingstjenester, er blant annet gitt i lov av 23. mai 2003 nr. 35 om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven). Ehandelsloven gjelder for elektronisk handel og andre informasjonssamfunnstjenester og offentlige myndigheters regulering av, og kontroll med, slike tjenester, jf. lovens § 1 første ledd. En informasjonssamfunnstjeneste er definert som «enhver tjeneste som vanligvis ytes mot vederlag og som formidles elektronisk, over avstand og etter individuell anmodning fra en tjenestemottaker», jf. annet ledd bokstav a). I henhold til forarbeidene til bestemmelsen, Ot.prp. nr. 31 (2002-2003) på side 56, vil nettbanktjenester omfattes. Følgende er uttalt:

> «En tjeneste er ikke formidlet elektronisk dersom innholdet er materielt selv om det innebærer bruk av elektroniske innretninger, for eksempel penge- eller billettautomater (pengesedler og togbilletter). Dette betyr bl.a. at å ta ut penger i en minibank ikke er en informasjonssamfunnstjeneste, men overføring av penger ved bruk av Internettbank vil være en slik tjeneste.»

Ehandelsloven § 11 om opplysningsplikt før elektronisk bestilling, har fastsatt bestemmelser som direkte vedrører inntastingsfeil. I henhold til bestemmelsens første ledd bokstav d), skal tjenesteyteren, før elektronisk bestilling, på en klar, forståelig og utvetydig måte gi tjenestemottakeren opplysning om «de tekniske midlene til å finne og rette inntastingsfeil før bestilling er foretatt». I forarbeidene til bestemmelsen, Ot.prp. nr. 31 (2002-2003) side 63, er det uttalt at:

> «Når avtaleinngåelsen teknisk er tilrettelagt slik at mottakeren kan finne og rette feil vil mottakeren føle seg tryggere i avtalesituasjonen. Videre motvirker dette at feil oppstår og at noen blir forpliktet uten å måtte ønske dette».

Etter tredje ledd er det videre bestemt at tjenesteyteren «skal tilrettelegge den elektroniske avtaleinngåelsen slik at inntastingsfeil på en enkel måte kan oppdages og rettes før avtalen inngås». På side 63 i proposisjonen er det sagt at denne bestemmelsen er et supplement til bokstav d) og skal gjøre

> «avtaleinngåelsen enklere og mer betryggende for tjenestemottakeren. Det antas at bestemmelsen kan oppfylles ved å gi tjenestemottakeren en oversikt over hva som er bestilt og hvilke opplysninger som er gitt før endelig ordre sendes til tjenesteyteren».

I forhold til de eksisterende nettbanktjenestene i markedet er situasjonen at tjenestemottakeren har tilgang til en slik oversikt. Dersom kunden legger inn et betalingsoppdrag, vil det automatisk komme opp et nytt vindu hvor kunden må bekrefte den allerede inntastede informasjon før betalingen kan bli behandlet i bankens system for betalingsoverføring. Dette var også en av anbefalingene fra Bankenes Standardiseringskontor for å øke kundenes trygghet i bruk av sine nettbankløsninger, se avsnitt 1.3 foran.

I forhold til den type feil som drøftes i denne omgang, nemlig kundens egne feil i form av særlig feiltasting uten at dette oppdages før betalingsoppdraget iverksettes, må det derfor legges til at nettbanktjenestene tilfredsstiller kravene etter ehandelsloven. Lovens § 15 om erstatnings- og straffeansvar for tjenesteytere er derfor ikke aktuelt for bankinstitusjonene som tilbyr nettbanktjenester. Utover kundefeilene kan det imidlertid ikke utelukkes at ehandelslovens regler om erstatningsansvar vil kunne komme til anvendelse. Banklovkommisjonen går imidlertid ikke nærmere inn på dette spørsmålet.

5.5.5 Bestemmelser i betalingssystemloven

Betalingssystemloven av 17. desember 1999 nr. 95 kan også være av betydning i denne sammenheng. I brev fra Justisdepartementet til Finansdepartementet av 31. oktober 2006 om sikkerhet ved bruk av nettbank, hvor det blant annet ble gitt en vurdering av spørsmålet om en mulig ansvarsbegrensning for nettbankkunder dersom det oppstår tap som følge av feil fra kundens side, uttalte departementet, på side 2, følgende:

> «Vi vil anta at institusjonen etter omstendighetene for eksempel kan bli ansvarlig dersom den tilbyr et betalingssystem som ikke tilfredsstiller grunnleggende krav til sikkerhet mv. Vi viser i den forbindelse til betalingssystemloven § 3-1, som slår fast at «systemer for betalingstjenester [skal] innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas».»

Betalingssystemloven kommer blant annet til anvendelse på systemer for betalingstjenester som er basert på standardvilkår for overføring av penger fra eller mellom kundekonti i banker og finansieringsforetak når overføringene bygger på bruk av betalingskort, tallkoder eller annen form for selvstendig brukerlegitimasjon utstedt til en ubestemt krets, jf. lovens § 1-1 annet ledd og kapittel 3. Loven har imidlertid ingen nærmere regulering av ansvarsforholdet mellom kunde og institusjon dersom kunden gjør en feil som leder til et økonomisk tap. I lovens § 3-1 er det for så vidt fastslått at systemer for betalingstjenester skal «innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utføring av betalingstjenester ivaretas». I dette ligger antageligvis at institusjonen etter omstendighetene kan bli ansvarlig dersom den tilbyr et betalingssystem som ikke tilfredsstiller grunnleggende krav til sikkerhet mv. Bestemmelsen kan også ha betydning i forhold til tredjemanns misbruk, men denne vinklingen er utelatt i denne sammenheng.

Feil som er gjort av kunden selv ved overføring i nettbank, kan for det første ha sitt utspring i at betalingssystemet ikke tilfredsstiller grunnleg-

gende krav til sikkerhet. I et slikt tilfelle kan det være aktuelt å ilegge institusjonen ansvar dersom det oppstår feilbruk som systemet burde oppdaget og rettet. I henhold til lovens § 3-1 er det, som sitatet foran viser, slått fast at systemer for betalingstjenester skal innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas.

Banklovkommisjonen har i sin Utredning nr. 3 (NOU 1996: 24 Betalingssystemer m.v.) uttalt at gode kontrollrutiner er viktige for å oppnå «sikker betalingsoverføring» og for at systemet skal oppnå nødvendig tillit blant brukerne. Kontrollrutinene må være innrettet for å hindre og avsløre feil, misbruk og manipulering i systemene. Slike feilkilder er bare delvis regulert i finansavtaleloven. Dette vedrører først og fremst feil fra institusjonens side og misbruk fra tredjemenn, se finansavtaleloven kapittel 2 IV og V. Finansinstitusjonene generelt, og bankene spesielt, har inngått avtaler hvor det er fastlagt alminnelige systemkrav som dekker flere av de sentrale elementer i formålsbeskrivelsen. Det er også lagt opp til at Kredittilsynet kan gi nærmere regler om standardisering av avtaler, vilkår, tekniske forhold mv. for systemer for betalingstjenester, jf. betalingssystemloven § 3-3 første ledd annet punktum. Denne regelen ble inntatt for å sikre at alle elementene i formålsbestemmelsen dekkes på en tilfredsstillende måte. Med hjemmel i blant annet denne bestemmelsen har Kredittilsynet fastsatt en forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) av 21. mai 2003 nr. 630. Forskriften gjelder for en rekke norske finansinstitusjoner, jf. forskriften § 1. I forskriftens § 5 om sikkerhet er det bestemt at foretak som omfattes av forskriften skal

> «utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk».

Videre er det bestemt at foretaket skal sikre at IKT-systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift, jf. forskriften § 7. De ovennevnte reglene, både i lov og forskrift viser at det stilles strenge krav til foretak som tilbyr systemer for betalingstjenester. Ved feil forårsaket av kunden selv kan det derfor statueres et erstatningsansvar for foretaket, dersom det ikke er etablert tilfredsstillende kontrollrutiner som kan oppdage slike feilkilder. Det foreligger likevel begrenset norsk rettspraksis på dette området og det er vanskelig å kunne si noe sikkert om utfallet av den enkelte sak. De nåværende tiltakene som er iverksatt av næringen, jf. avsnitt 1.3 foran, vil langt på vei hindre at det oppstår slike tilfeller og vil kunne påberopes av institusjonene i spørsmål om ansvarsplassering dersom det har oppstått et tap som følge av kundens feiltasting eller lignende. Et eventuelt ansvar vil nødvendigvis være gjenstand for flere vurderingstemaer og momenter. Det er også sannsynlig at et ansvarsgrunnlag i tillegg må forankres i hensyn som begrunner det ulovfestede objektive ansvaret, se avsnitt 5.5.7 nedenfor.

5.5.6 Øvrige bestemmelser

Banklovkommisjonen finner også grunn til å nevne avtaleloven § 32 om feilskrift ved viljeserklæringer. Bestemmelsen legger opp til at feiltakelser fra den som avgir viljeserklæringen, ikke er bundet av dets innhold dersom mottager «indsaa eller burde indse, at der forelaa en feiltagelse», jf. bestemmelsens første ledd i.f. Det kan her stilles spørsmål ved om bestemmelsen oppstiller krav til institusjoners aktpågivenhet med henhold til å oppdage eventuelle utilsiktede betalingsoppdrag fra kundens side. På den annen side må dette forhold knyttes opp mot de krav som er stilt til institusjonene i kraft av ehandelsloven, som er gjennomgått foran avsnitt 5.5.4. Etter *Banklovkommisjonens* oppfatning er det mye som taler for at institusjonene, ut fra de sikkerhets- og kontrolltiltak som er iverksatt i forbindelse med betalingsoverføringer, som hovedregel ikke kan sies å være i ond tro ved utilsiktet avvik i en kundes initiering av et betalingsoppdrag.

5.5.7 Alminnelige erstatningsregler

Det neste spørsmålet blir om banken kan holdes ansvarlig etter alminnelige erstatningsregler.

Det er forskjellige former for ansvarsregler som her kan tenkes å komme til anvendelse.

1) Først bør det sies at nettbanktjenesten har et preg av å være en genusvare uten at *Banklovkommisjonen* finner grunn til å gå nærmere inn på en slik drøftelse. For genuskjøp har det lenge vært hevdet å foreligge et kontrollansvar i forbindelse med kontraktsbrudd fra tjenesteyters side. Videre er det samme lagt til grunn i juridisk teori om betalingsformidling. I Olav Torvund, Betalingsformidling, 1993, på side 324, er følgende uttalt om ansvarsgrunnlaget for betalingsformidleren:

> «I en type [betalings]tjeneste hvor man er avhengig av komplisert teknikk og sikre rutiner, og hvor tjenesteyter kontrollerer systemet, synes kontrollansvar å fremstå som en hensiktsmessig løsning. Det fokuseres mer på at

> den som har kontroll over systemene og rutinene har ansvaret for at disse er gode nok, enn på om noen har opptrådt uaktsomt. Risiko blir mer fremtredende enn skyld. Den vurdering som kontrollansvaret legger opp til, er mer realistisk enn et skyldansvar med omvendt bevisbyrde og strenge krav til bevis.»

Dersom dette legges til grunn, blir det neste spørsmålet hvilke omstendigheter som skal kunne frita for ansvar i forbindelse med feiltasting fra kundens side. Det er antatt at banken vil være ansvarlig for svikt i rutiner og annen teknisk svikt mv. Med andre ord vil det kunne statueres ansvar dersom banken ikke har gjort det som var mulig å gjøre for å unngå feilen. Dette er et vanskelig vurderingsspørsmål og vil bero på en rekke faktorer. Det kan hevdes at bankinstitusjonene bør foreta en forsvarlig brukertesting. Med dette menes at det er utviklet et tilfredsstillende brukergrensesnitt, det vil si at det finnes mekanismer som kontrollerer inntasting og gir feilmeldinger og advarsler dersom ikke alt ser ut til å stemme i relasjonen mellom menneske og maskin. Sentrale krav til brukergrensesnitt vil typisk gjelde:

1. Grensesnittet skal understøtte brukeren i å utføre oppgaven.
2. Grensesnittet skal vise tilstanden til systemet, slik at brukeren til enhver tid har oversikt over situasjonen.
3. Kommandoer fra brukeren, som tastetrykk og inntasting, skal reduseres til et minimum og foregå mest mulig effektivt.
4. Systemet skal detektere alle feil som er mulig å oppfange.
5. Systemet skal redusere konsekvensen av feil.[21]

Slikt brukergrensesnitt er i stor grad lagt til grunn for nettbanktjenesten, jf. også tiltakene fra næringen. Det kan imidlertid stilles spørsmål ved om inntastingsfeil er forhold som er så nærliggende ved kundens bruk av systemet at dette skal anses som en feil som på et eller annet vis bør kunne plukkes opp av systemet. For eksempel kan feil datoangivelse for belastning av oppdraget tastes inn feil. Dette kan medføre økonomisk tap for kunden, jf. avsnitt 5.4.1 foran. Her kan det tenkes at visse nettbanktjenester har forskjellige kontrollmekanismer for å oppdage utilsiktede datoangivelser, for eksempel at inntasting av årstall ett år frem i tid medfører at det kommer en melding om at betalingsoppdraget ikke skal belastes før om ett år.

Banklovkommisjonen har imidlertid ikke funnet grunn til å konkludere om kontrollansvaret vil kunne legges til grunn i de tilfeller hvor tap har oppstått som følge av feil fra kundens side. Oppfatningen synes å være at man befinner seg på et usikkert rettsområde hvor en særlig lovregulering uansett bør vurderes. En gjennomgang av øvrige aktuelle erstatningsregler er likevel hensiktsmessig for å danne seg et helhetlig bilde av rettstilstanden.

Dersom man kommer til at banken ikke kan holdes ansvarlig etter kontrollansvarsregelen, nevnes at et nærliggende spørsmål vil være om kundens ansvar skal lempes, sml. kjøpsloven § 70 annet ledd.

2) Spørsmålet er videre om tap som følge av kundens feilbruk skal bæres av institusjonen etter reglene om objektivt erstatningsansvar. Utgangspunktet er at når et selskap driver virksomhet med særlige risikoaspekter, bør selskapet dekke følgene av eventuelle tap som kan oppstå som følge av denne virksomheten. Nettbanktjenesten er et teknisk komplisert system som innebærer en risiko for at det oppstår kundefeil og økonomisk tap for denne.

I brevet fra Justisdepartementet av 31. oktober 2006 om sikkerhet ved bruk av nettbank, se avsnitt 5.5.5 foran, fastslo departementet, på side 2, at ansvar for kundens egne feil som følge av at betalingssystemet ikke tilfredsstiller grunnleggende krav til sikkerhet mv. også delvis vil

> «kunne forankres ut fra de hensyn som begrunner det ulovfestede objektive ansvaret. Videre kan nok ansvar i en del tilfeller begrunnes i at institusjonen har etablert prosedyrer eller rutiner som er egnet til å misforstås av kunden. Et eksempel på det siste er Bankklagenemndas avgjørelse BKN-05087, hvor kunden hadde betalt et fakturabeløp to ganger (til et firma som senere var gått konkurs). Kunden hadde misforstått instruksjonen i telefonbanken, og belastet både sparekontoen og brukskontoen for beløpet. Bankklagenemnda kom til at banken burde dekke halve tapet, og uttalte blant annet følgende som begrunnelse for dette:
>
> «Bankklagenemnda har gjennomgått rutinebeskrivelsen, som viser hvilke instrukser klager fikk over telefonen, og hvilke valg hun foretok. Etter nemndas oppfatning kan instruksen ikke sies å være selvforklarende på det avgjørende punkt. (...) Banken opplyser at den for en tid tilbake foretok en endring av systemet. Dette ledet til en endring av rutinen i forhold til den som tidligere gjaldt, nemlig at kunden alltid måtte taste det kontonummeret som skulle belastes. (...) Den uklarhet som er oppstått, og som er bakgrunnen for klagers handle-

[21] Jf. rapport fra professor Kai A. Olsen fra Høgskolen i Molde: «Inntasting i nettbank» side 7.

måte i det aktuelle tilfellet, må etter dette langt på vei sies å være skapt av banken.»

Et synspunkt som også kan statuere et objektivt ansvar for en virksomhet, i dette tilfelle for institusjoner som tilbyr nettbanktjenester, er interesseavveiningssynspunktet. Det går ut på at virksomheter som for omverden representerer en risiko eller fare, og som gir driftsherren økonomisk gevinst, selv bør bære de skadene den volder, idet disse kan inngå som en omkostning ved produksjonen. I NOU 1980: 29 Produktansvaret, blir et objektivt ansvar blant annet begrunnet på denne måten (s. 83):

«De skader som produktet måtte volde, bør anses som en normal produktkostnad som bør belastes produktet, og ikke den som tilfeldig rammes av en skade. Denne risiko blir en kostnad som må tas i betraktning ved produktets markedsføring, og den kan normalt dekkes ved forsikring og er således kalkulerbar».

Videre blir det ofte fremhevet at en regel om objektivt ansvar medfører at risikoen for at det oppstår et økonomisk tap legges hos den som normalt har den beste økonomiske bæreevne. I USA hevdes det ofte at en av erstatningsrettens viktigste oppgaver er å plassere risikoen hvor tapet best kan bæres («the deep pocket justification»). Dette tilsier at ansvaret i stor utstrekning legges på produsentene. Erstatningsplikten blir da en driftsomkostning som i siste omgang må bæres av virksomhetens kunder. Dette leder således frem til en pulverisering av tapet.

Muligheten til å pulverisere tapet som en omkostning i sin videre drift er således et viktig moment, se også Rt. 1992 s. 64 hvor det ble uttalt at tapet «for de få brukere som rammes katastrofalt, bør dekkes av produsenten som kan kalkulere dette som en omkostning». Overført på nettbanktjenestene, må det i denne sammenheng sies, at et eventuelt ansvar for institusjonen ved oppstått tap må bedømmes i hvert konkrete tilfelle. I tillegg vil risikoelementene ved bruk av nettbank stadig forandre seg. I den sammenheng kan det vises til produktansvarsloven av 23. desember 1988 nr. 104 § 2-1. Her er det bestemt at produsenten

«plikter å erstatte skade som hans produkt volder og som skyldes at det ikke byr den sikkerhet som en bruker eller allmennheten med rimelighet kunne vente (heretter kalt sikkerhetsmangel). Ved vurderingen av den sikkerhet som kan ventes, tas hensyn til alle forhold som har sammenheng med produktet, dets presentasjon, markedsføring og påregnelige bruk».

Det er uansett ikke like selvsagt at institusjonen skal bære hele tapet ved kundens inntastingsfeil, dersom kunden ut fra en vurdering, ikke kan sies å ha opptrådt aktsomt og varsomt nok i den videre prosesseringen av betalingsoverføringen, for eksempel ved at betalingsoverføringen er bekreftet i et nytt vindu, sml. Bankklagenemndas uttalelse i BKN-07106, samt forarbeidene til ehandelsloven § 11 nevnt i avsnitt 5.5.4 foran. Her blir spørsmålet om bankens ansvar skal nedsettes eller falle bort som følge av skadelidtes medvirkning.

På den annen side har praksis i nettbankene vist at inntastingsfeil ikke skjer i et stort omfang. Feilprosenten kan slik sett sies å være lav, men tatt i betraktning det høye antallet av nettbanktransaksjoner, er risikoen likevel klart fremtredende. Dette er et moment som ut fra en pulveriseringstankegang, kan lede til at nettbanken likevel må anses ansvarlig på objektivt grunnlag. I saken om bankkunden som feilaktig overførte 500.000 kroner til en uvedkommende, ble det inngått forlik blant annet ut fra at det nettopp dreide seg om en engangshendelse. Med de nye tiltakene som er iverksatt for å trygge sikkerheten ved bruk av nettbanktjenesten, se avsnitt 1.3 foran, er det imidlertid lite som taler for at en lignende sak med et lignende utfall vil kunne oppstå igjen. Normalavvik eller feilbruk kan likevel manifestere seg på andre måter. Det kan tenkes et mangfold av samvirkende årsaker og forhold som må vurderes i hver enkelt sak.

Ansvarsplasseringen kan i en del tilfeller bli bestemt av at institusjonen har etablert prosedyrer eller rutiner som er egnet til å misforstås av kunden, jf. også brevet fra Justisdepartementet. Et eksempel på det siste er Bankklagenemndas avgjørelse BKN-05087, hvor kunden hadde misforstått prosedyren for gjennomføring av telegirobetaling, som ledet til at kunden betalte samme fakturabeløp to ganger. Den uklarhet som var oppstått, måtte langt på vei sies å være skapt av banken. Kunden burde imidlertid ha foretatt undersøkelser da hun registrerte transaksjonene, til tross for at hun hadde fått en betalingsbekreftelse over kontofonen, ikke var gjennomført som antatt. Nemnda kom til at tapet burde deles mellom partene. Ved telefonbank, foretas kontroll med betalinger på auditiv måte, mens det ved nettbank foretas en visuell kontroll. Det vil måtte vurderes om risikoen for feilbruk er større ved auditiv enn visuell kontroll, men Bankklagenemndas avgjørelse vil ha en viss overføringsverdi for feilbruk i nettbank.

Det er videre flere momenter som er av betydning i forhold til å kunne statuere ulovfestet objektivt ansvar for bankinstitusjonen som tilbyr nett-

banktjeneste. Tre av dem står mer sentralt enn andre. For det første gjelder det risikoens størrelse eller omfang; den må i vesentlig grad overstige «dagliglivets risiko». Videre at risikoen, for det andre, må være stadig og, for det tredje, typisk, se Peter Lødrup, Erstatningsrett, 1999, side 248 flg. Nyere rettspraksis synes imidlertid å legge mer vekt på risikoen for skade, enn at den skal være stadig og typisk. Derimot må det nok stilles som krav at risikoen er ekstraordinær. Skadelidte skal videre vernes mot en risiko som han ikke kunne eller burde være forberedt på eller påregne. Det er ikke tvilsomt at objektivt ansvar også kan pålegges hvor det er meget sjelden at skade inntreffer, eller hvor en slik skade ikke har inntruffet før, men at det tross alt er noe man må regne med kan skje. Det er da muligheten for at en alvorlig skade kan inntre som i hovedsak begrunner ansvaret, ikke hyppigheten av skader ved vedkommende virksomhet.

Et annet sentralt tema er at skaden må være en typisk og påregnelig (nærliggende) følge av virksomheten. Hvis den skadevoldende innretning kunne vært gjort sikrere ved enkle midler, eller hvor et annet nærliggende handlingsmønster kunne forhindret skaden, taler dette for å pålegge objektivt ansvar. Er det mulig å fjerne risikoen helt, eller å gjøre den skadevoldende innretning sikrere ved enklere midler, taler også dette for objektivt ansvar. Tankegangen er at et objektivt ansvar oppfordrer til sikkerhetstiltak – reparasjoner, inspeksjoner, tekniske forbedringer og lignende – for å hindre at skade inntrer, selv om unnlatelsen av å gjøre dette ikke kan betegnes som uaktsom. Er skaden imidlertid voldt i forbindelse med handlinger som også er foretatt i skadelidtes interesse, vil avveiningen lettere slå ut i skadevolderens favør, selv om mange av de momenter som ellers taler for et objektivt ansvar er til stede. Videre har skadelidtes forhold innflytelse på spørsmålet om det bør pålegges objektivt ansvar, også i forhold til en eventuell erstatningsutbetaling, se skadeserstatningsloven av 13. juni 1969 nr. 26 § 5-1. Aksept av risiko innebærer eksempelvis at man ikke kan vernes av det objektive ansvar når man ved sin handlemåte eller virksomhet må sies å ha akseptert den risiko som begrunner dette ansvaret.

Som gjennomgangen viser, er det mange momenter å ta hensyn til i forhold til spørsmålet om institusjonen skal kunne pålegges ansvar ved oppstått tap som følge av kundens feilbruk av nettbanktjenesten. Det er imidlertid ikke *Banklovkommisjonens* oppgave å komme til bestemte konklusjoner på dette området. Formålet her har vært å gi en oversikt over gjeldende rett som kan tjene som et utgangspunkt for en nærmere vurdering av lovgivningsbehovet og en vurdering av hovedelementene i en mulig ansvarsregulering i tilfelle hvor kundens handlemåte avviker fra normal opptreden i sin bruk av nettbanktjenesten.

5.6 Risiko for andres misbruk

5.6.1 Innledning

Til ethvert betalingsoverføringssystem med brukerlegitimasjon som det avgjørende tilgangskriteriet, vil det alltid foreligge en risiko for misbruk fra utenforstående. Dette forsterkes ytterligere i forhold til systemer for betalingstjenester som er tilgjengelige i åpne nettverk som for eksempel Internett. Risikoen for uautorisert bruk eller adgang er knyttet til flere forhold. Dette omfatter vanligvis hvor høy grad av sikkerhet som kreves i forhold til tilgangskontroll og pålogging (autorisasjon og autentisering), og i hvilken grad den datamaskin som anvendes mot betalingstjenesten er beskyttet (brannmur og antivirus-programmer mv.).

Erfaringene fra tilfeller med misbruk av betalingskort viser at en praktisk viktig gruppe henspeiler seg på situasjoner hvor tredjemanns tilgang til nødvendig brukerlegitimasjon kan tilbakeføres til kundens egen oppbevaring av denne legitimasjonen. Denne gruppen av tilfeller vil også være aktuell i forhold til de nettbaserte betalingstjenestene ettersom det også her kreves brukerlegitimasjon for å kunne ta i bruk tjenesten. For øvrig vil trusselbildet når det gjelder nettbank generelt sett være et annet, og det vil til enhver tid også være i endring. Anvendelsesområdet for hjemme-pc og omfanget av tjenestetilbudet fra leverandører som anvender Internett som markedsplass for sine produkter og/eller tjenester er i stadig utvikling og skaper økt risiko for nye misbruksformer. Det som benevnes som «Web 2.0», det vil si nettsteder eller -samfunn som tilrettelegger for omfattende fildeling og tilbud om nedlastbare varer og tjenester, film og streaming mv. skaper nye muligheter for datainnbrudd og misbruk.

Innenfor nettbaserte systemer, uavhengig av om det dreier seg om betalingsoverføringer, har det tradisjonelt sett vært en stor fare for at uvedkommende påfører skade ved inntrenging eller «hacking» i slike systemer. Dette har særlig manifestert seg i ødeleggelse av databasesystemer, inntrenging i systemer for å tilegne seg informasjon, for eksempel militære hemmeligheter, og spredning av informasjon eller propaganda uten at det primære målet har vært å tilegne seg en direkte økonomisk gevinst. Det kan sies at hacking og

spredning av virus og annen ondsinnet koding/programvare tidligere ofte var begrenset til enkeltpersoner hvis hensikt var å oppnå status i spesielle miljøer. Med etablering av nettbaserte betalingssystemer, først og fremst ved bruk av internasjonale betalingskort ved netthandel, og nå andre nettbaserte betalingstjenester, har imidlertid det tradisjonelle bildet endret seg gradvis. Hacking foregår ofte nå i organisert form mot enkelte eller flere institusjoner samlet for å oppnå en økonomisk gevinst.[22] I takt med den teknologiske utviklingen kan det dessuten bli vanskeligere å gardere seg mot slike angrep.

Det at tredjemann skal klare å få tilgang til en nettbankkonto og på urettmessig vis disponere kontoen, har som oftest sitt utspring i en eller annen form for relasjon til kunden. Her må det skilles mellom misbruk via en kundes datamaskin og misbruk via tilegnelse av en kundes tilgangsopplysninger. Sistnevnte misbrukssituasjon dekker hacking på en kundes datamaskin eller telefon, samt de tradisjonelle formene for urettmessig tilegnelse av informasjon via innbrudd i postkasse, bopel eller lignende til kunden. Disse misbruksmulighetene henger imidlertid i stor grad sammen. Fellesnevneren er at kunden blir lurt og/eller misbrukt av en utenforstående. Trusselbildet er slik sett sammensatt, ettersom tjenesten dekker så bredt og griper inn på flere forhold i kundens private sfære. I forhold til alle former for misbruk er det bare fantasien som setter grenser for typetilfellene. Teknologien og svindlernes tilnærmingsmåter er dessuten av dynamisk karakter og legger grunnlag for stadig nye svindelmuligheter.

Det vil alltid være mulig å finne sårbarheter i sikkerhetsløsninger. Slik sett vil det også alltid foreligge en risiko for at det forekommer misbruk, enten ved at en kunde går frem på en måte som avviker fra normale prosedyrer eller fører til urettmessige transaksjoner, enten i forbindelse med oppbevaring av kode, bruk av datamaskin som ikke har oppdaterte virusprogrammer eller lignende, elektronisk kontakt med uvedkommende som forsøker å få kundens tilgangsopplysninger mv. I det følgende gjennomgås potensielle misbrukssituasjoner i forhold til både nettbank- og telefonbanktjenester.

[22] Det nevnes for eksempel det antatte datainnbruddet mot Best Western i slutten av august 2008, hvor man frykter at kredittinformasjon til flere tusen kredittkortkunder er kommet på avveie og solgt til kriminelle nettverk. Dette medførte at et stort antall kredittkort ble sperret av de berørte kredittkortselskapene.

5.6.2 Nettbank

Ettersom misbruksmulighetene er mange, har *Banklovkommisjonen* funnet det hensiktsmessig å oppdele beskrivelsen av risiko for andres misbruk ved bruk av nettbank. Som nevnt i avsnitt 5.6.1 foran, bunner misbruk av nettbankkonto ut i en eller annen form for relasjon til kunden. I første omgang beskrives risikoen for misbruk gjennom det som kan kalles tradisjonell fremgangsmåte. Dette dekker først og fremst falsk legitimering ved henting av sikkerhetsverktøy (koder mv.) og innbrudd i postkasse eller bopel, se punkt 1). I andre omgang beskrives de nyere og mer avanserte formene for misbruk av en kundes bankkonto. Dette kan kalles for misbruk via nettbaserte fremgangsmåter, se punkt 2). Her er det et bredt spekter av risikosituasjoner og mange tenkelige kombinasjoner av fremgangsmåter. Banklovkommisjonen nevner de som er ansett som viktigst på nåværende tidspunkt, men utelukker ikke at nye og mer effektive former vil oppstå.[23]

1) *Tradisjonell fremgangsmåte.* Misbruk av en kundens nettbankkonto kan forekomme ved at tredjemann får tak i tilgangsopplysninger allerede før kunden selv har tatt i bruk nettbanken. Dette forutsetter for så vidt at kunden allerede har et etablert kundeforhold og konto i banken som nettbanktjenesten knyttes opp mot. I andre tilfelle, for eksempel ved de rene nettbaserte bankene, vil det jo som oftest ikke være midler på kontoen før kunden selv har tatt den i bruk. Slikt misbruk kan skje ved postinnbrudd i kundens postkasse, hvor PIN-kode sendes, og at gjerningspersonen møter opp på postkontoret og fremviser falsk legitimasjon for å få utlevert nødvendig sikkerhetsverktøy til nettbanken.

Når kunden har opprettet nettbankkonto, kan misbruk også forekomme ved postinnbrudd. Som nevnt i avsnitt 5.2.1 foran, vil engangskodeverktøyet sendes direkte til kundens bopel dersom det er utgått eller kunden har mistet det. Dette forutsetter for øvrig at gjerningspersonen urettmessig har tilegnet seg kundens PIN-kode, for eksempel ved hjelp av nettbaserte fremgangsmåter, jf. punkt 2) nedenfor.

Misbruk kan videre skje ved at tredjemann bryter seg inn i kundens bopel og tilegner seg nødvendig brukerlegitimasjon, både kode og engangskodeverktøy. Selv om det i kontoavtalene er forutsatt at kunden ikke skal notere ned sin personlige kode, herunder BankID, kan det ikke utelukkes at

[23] For en bredere redegjørelse av dette temaet, viser Banklovkommisjonen til utredning fra Datakrimutvalget i NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.4 følgende.

dette faktisk gjøres i større eller mindre grad blant dagens nettbankkunder. Dette er det også sett eksempler på i rettspraksis, jf. avsnitt 5.7.3 nedenfor.

2) *Nettbasert fremgangsmåte.* Misbruk kan også forekomme som følge av kundens tilknytning til Internett, herunder oppkobling direkte mot sin bank og bankkonto. Her er det mange forskjellige situasjoner som kan lede til at misbruk oppstår. Før det gis en oversikt over noen av de potensielle misbrukstilfellene, bør det sies at Internett gir store muligheter for å operere internasjonalt og under falsk identitet, slik at de potensielle farekildene ikke nødvendigvis trenger å være lokale.

En potensiell misbrukssituasjon er at tredjemenn «hacker» eller trenger seg inn i kundens datasystemer. Dette datainnbruddet innebærer at gjerningspersonen skaffer seg adgang til et datasystem hvor vedkommende ikke har rettmessig adgang. Det er flere konsekvenser av et slikt datainnbrudd. Det som er særlig aktuelt i forhold til misbruk av nettbanktjenesten er at dataene som er lagret på systemet (for eksempel nødvendige tilgangskoder mv.) blir kjent for uvedkommende. Ettersom dagens pålogging i nettbank forutsetter oppgivelse av genererte engangskoder, er ikke slike datainnbrudd like faretruende lenger. Inntrenging i systemet og overtakelse av en kundes nettbanksesjon er imidlertid en risiko. Denne form for misbruk kalles for «man-in-the-middle» og beskrives nedenfor.

Videre er det mulig å befeste kundens datamaskin med en uønsket programvare som utgir seg for noe annet, gjerne et nyttig program som i tillegg til (eller i stedet for) nyttige funksjoner inneholder programkode som gir gjerningspersonen tilgang til datamaskinen. Ved siden av nettsteder som kun er opprettet for å spre slike programvarer, har risikoen for slike virus tradisjonelt sett vært stor på pornografiske nettsteder og nettsteder for spill og gambling. Den siste tiden har imidlertid slike virus i stor grad blitt spredd via statlige og kommunale nettsteder, i tillegg til andre mer normale nettsteder, se nedenfor. Denne programvaren kan «bli med inn» i kundens sesjon med nettbanken og lede til urettmessig disponering av kundens konto (såkalt «trojansk hest»). De mest avanserte programvarene gjør det dessuten mulig for angriperen å utføre en rekke funksjoner på kundens datamaskin, for eksempel lese filer, lure til seg passord og koder, overvåke skjermbildet eller avlytte rommet med datamaskinens mikrofon. Dette er en slags spionprogramvare som uberettiget overvåker eller samler inn informasjon fra en datamaskin, jf. for så vidt beskrivelsen foran om tilfeller hvor kundens maskin blir utsatt for hacking. Ondsinnede programvarer kan også implementeres i fiktive reklamekampanjer på «chatte»-nettsteder, for eksempel MSN.[24] Slik implementering kan også gjøres i musikk- og filmfiler som ulovlig deles på Internett (piratomsetning). Slike ulovlige virksomheter er for så vidt i stor grad knyttet opp til masseutsendelse av «spam» eller «søppelpost» uten at *Banklovkommisjonen* finner grunn til å gå nærmere inn på dette.[25] Ellers kan det nevnes at det nylig er avslørt sikkerhetsmangler ved større online spill. Dette er såkalt «massive multiplayer online game» (MMO) hvor flere tusen personer kan spille samtidig. Svakheter i kodingen ved spillene har gjort det mulig for uvedkommende å lese vilkårlige filer på andre deltakeres datamaskiner. Dette kan omfatte sensitiv og personlig informasjon, slik som passord og kontoopplysninger.[26]

Et «man-in-the-middle»-angrep er en annen form for misbrukstrussel. Dette innebærer at angriperen kan lese, redigere og modifisere beskjeder mellom to kommuniserende parter uten at noen av partene er klar over at det foregår. Dette forutsetter at angriperen har fått tilgang til kundens datasystemer og kan være en konsekvens av eksempelvis en «trojansk hest» som nevnt foran. Angriperen må få muligheten til å observere og avskjære beskjeder mellom to ofre. Overført på nettbanktjenesten vil dette si at kunden tror han sender en beskjed til banken om et konkret betalingsoppdrag. Dette oppdraget blir imidlertid modifisert før det sendes til banken. Banken mottar det modifiserte betalingsoppdraget og utfører transaksjonen i henhold til dette. Banken sender deretter beskjed tilbake til kunden som underveis blir modifisert slik at kunden tror det opprinnelige betalingsoppdraget er utført på korrekt vis. Et slikt angrep krever forholdsvis store ressurser og avanserte programvarer som kan kryptere den informasjon som sendes mellom partene meget raskt. Dette gjelder dess mer i de nettbanker hvor hver enkelt betalingsoverføring forutsetter bruk av en engangskode.

En kundes datamaskin kan videre bli manipulert av en utenforstående tredjemann slik at det gis feil oppdrag til banken (såkalt «fantomtransaksjon»). Dette kan eksempelvis manifestere seg i at kunden skriver tallet 1, men datamaskinen hans

[24] Se artikkel på vg.no av 27. august 2008 med overskrift «Trojaner på MSN.no».

[25] Se ellers NOU 2007: 2 Lovtiltak mot datakriminalitet avsnitt 3.6.

[26] Undersøkelsen og oppdagelsen ble utført av Independent Security Evaluators (ISE) i august 2008, se securityevaluators.com.

eller hennes sender tallet 2. Det kan også forekomme tilfeller hvor kundens datamaskin på egen hånd prosesserer et oppdrag til banken. Dette forutsetter for øvrig at kunden ikke har avsluttet sin sesjon med nettbanken. Så lenge kunden ikke logger ut av banken vil angriperen kunne prosessere flere oppdrag til banken, ettersom sesjonen blir ansett som aktiv og bankens sikkerhetsmekanismer for tidsavbrudd ikke aktiviseres.[27] For de nettbanktjenester hvor det må tastes inn en engangskode for hvert betalingsoppdrag, reduseres imidlertid risikoen for slikt misbruk.«Phishing» er en annen svikfull fremgangsmåte som kan medføre misbruk av en bankkonto. Slikt misbruk er blitt definert som «an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging.»[28] Dette har særlig vært brukt i forbindelse med misbruk av betalingskort, men er også aktuelt for misbruk av nettbanktjenesten. «Phising» innebærer at tilgangsinformasjon fra kunden urettmessig tilegnes og benyttes til å disponere brukerens konto i nettbanken. For eksempel kan en bruker motta en e-post fra det som synes å være administrasjonen hos DnB NOR,[29] hvor det informeres om at det har oppstått et problem i bankens nettbankdatabase. Kunden blir bedt om å oversende sin brukerinformasjon på nytt med kode osv. Slike framgangsmåter er imidlertid blitt mindre effektive som følge av bankenes nye systemer med engangskoder (via engangskodeverktøy) som ved siden av innloggingsprosessen ofte må benyttes for registrering av hvert enkelt betalingsoppdrag.

Opprettelse av fiktive nettbankadresser kalles «website spoofing». Dette innebærer at det eksempelvis opprettes en fiktiv nettbankside som tilsvarer den virkelige nettbanksiden. Her blir kunden for eksempel bedt om å inntaste sin kode, PIN-kode eller personlig kode som ved BankID, som vanlig og deretter engangskode fra tildelt sikkerhetsverktøy. Tredjemann sitter et annet sted på bankens vanlige hjemmeside og taster inn kodene som brukeren avgir til vedkommende. Engangskoder som mottas per sms kan slik sett anses som en mer betryggende inngangsprosedyre siden dette er en engangskode som avløses ved at brukeren logger seg inn på bankens faktiske hjemmeside. Tredjemann kan imidlertid, gjennom ondsinnede programvarer ha muligheten til å overvåke en kundes mobiltelefontrafikk, slik at utsendelse av slike engangskoder også kan tilegnes på urettmessig vis. Risikoen her vil variere alt etter hva slags mobiltelefon som kunden bruker og sikkerhetsprogrammer som er installert i telefonen, jf. avsnitt 5.6.3 nedenfor.

Som følge av de risikoelementene som eksisterer i forhold til bruk av nettbank, tilbyr mange av bankene gratis antivirus- og brannmurprogramvare til sine kunder. Det oppfordres også til at brukerne oppdaterer sine nettlesere og undersøker om leverandøren til brukers operativsystem har lagt til rette for sikkerhetsoppdateringer, se avsnitt 5.7.2 nedenfor.

5.6.3 Telefonbank

I forhold til telefonbanktjenesten, gjelder mange av de samme risikoelementene. Det må her skilles mellom telegiro og mobilbank. Telegiro er ikke knyttet opp til Internett som mobilbank, og er ikke utsatt for de trusler som er gjennomgått under punkt 2) i avsnitt 5.6.2 foran. Telegiro, enten dette brukes fra fasttelefon eller mobiltelefon, er likevel knyttet opp til et telefonnettverk som tredjemann på urettmessig vis kan få tilgang til. I et leilighetskompleks bestående av en rekke fasttelefoner, vil «sistemann» på telefonleddet som går gjennom leilighetene med forholdsvis enkle ressurser ha mulighet til å avlytte samtalene og/eller identifisere tastetrykkene på telefonen.

For mobilbank foreligger det en utpreget risiko for at det oppstår misbruk. Som nevnt er mobilbank knyttet opp mot Internett slik at mange av de gjennomgåtte nettbaserte truslene for misbruk i forbindelse med bruk av nettbank også vil gjelde her. Risiko for slikt misbruk av mobilbank, forsterkes dessuten ved at mobiltelefoner ikke har samme velutrustede virus- og brannmurprogram som datamaskiner. En grunn til dette er at slike programmer krever stor kapasitet. Et stort antall av mobiltelefonene på markedet i dag som har tilgang til Internett har for så vidt begrenset kapasitet. Det er imidlertid utviklet nye og mer sikre systemer knyttet opp mot bruk av mobiltelefon som mobilbank, som for eksempel mobile signaturer.[30]

[27] Mekanismene for tidsavbrudd varierer fra bank til bank.

[28] Wikipedia.org.

[29] For å hindre at mottakeren kan undersøke hvem som er den egentlige avsender benyttes en teknikk som kalles «e-mail spoofing» hvor adressen til senderen og emne-feltet synes å komme fra eksempelvis DnB NOR, se også artikkel fra nordlys.no av 10. april 2008 med tittel ««Avsatte» Nordlys-redaktør».

[30] Dette systemet er basert på ETSI-MSS-standardene og er designet for bruk på mobiltelefon.

Videre er de nye sikkerhetsrutinene som er implementert for nettbanktjenestene også langt på vei overført i forhold til bruk av telefonbank, som for eksempel engangspassord, personlig passord mv. En helgardering mot misbruk, og for så vidt systemsvikt, er imidlertid et like vanskelig – og i noen tilfeller – et vanskeligere tema for telefonbank enn for nettbank. Det er dessuten grunn til å tro at det vil bli flere og hyppigere angrep mot denne plattformen fremover i takt med utvidelsen av tjenestetilbudet.

5.7 Ansvarsregulering ved andres misbruk

5.7.1 Innledning

Når det gjelder misbruk via en kundes datamaskin eller telefon, synes det å være et naturlig utgangspunkt at kunden identifiseres med sin egen datamaskin. Slik sett kan det hevdes at tredjemanns misbruk via en kundes datamaskin eller telefon i utgangspunktet er et forhold som kunden selv må lastes for, jf. alminnelige erstatningsregler. Her må det imidlertid tas hensyn til gjeldende ansvarsregulering i kontoavtalen og lovgivning, først og fremst finansavtaleloven, ved andres misbruk, jf avsnittene 5.7.2. og 5.7.3 nedenfor.

Det er særlig finansavtaleloven § 34 første ledd som danner utgangspunkt for denne reguleringen og selv om bestemmelsen er gjennomgått i avsnitt 2.6.2 foran, har *Banklovkommisjonen* ansett det hensiktsmessig å gjengi den her:

> «**§ 34**. *Misbruk av konto m.v.*
> (1) Kontohaveren er ikke ansvarlig for andres urettmessige uttak eller annen belastning med mindre den som har foretatt disposisjonen, har legitimert seg i samsvar med reglene i kontoavtalen, og belastningen har vært mulig som følge av forsett eller grov uaktsomhet fra kontohaveren eller fra noen som etter kontoavtalen har rett til å belaste kontoen.»

5.7.2 Kontoavtalen

Når det gjelder misbruk av konto, tilsvarer kontoavtalenes bestemmelser langt på vei finansavtalelovens regler, herunder særlig kapittel 2 V §§ 34 flg. om andres misbruk av konto og betalingsinstrument. En fremstiling av lovens § 34 er gitt i avsnitt 2.6.2 foran. I kontoavtalene er imidlertid visse forhold av betydning for ansvarsvurderingen etter bestemmelsen konkretisert. Det er eksempelvis fastslått at kunden er ansvarlig for at ikke uvedkommende får kjennskap til passordet. Videre at dersom det er benyttet korrekt passord, vil det bli lagt til grunn at det er kunden som har benyttet tjenestene. Dette er forhold som er klarlagt gjennom forarbeider og rettspraksis, men er likevel inntatt i mange av kontoavtalene.

I noen kontoavtaler er det også bestemt at institusjonen ikke er ansvarlig for tap som skyldes «ukorrekt bruk» hos kunden. Som eksempel er nevnt fullmaktsoverskridelser, men det er nærliggende å anta at «ukorrekt bruk» også vil kunne omfatte annen feilbruk hos kunden, som for eksempel at det ikke er installert tilfredsstillende sikkerhetsprogram på datamaskin som kunden benytter til å foreta betalingsoverføringer via nettbanktjenesten med.

Krav om slike sikkerhetsinnstillinger er for så vidt som oftest indirekte fastslått i de fleste kontoavtalene. I noen kontoavtaler er det bestemt at kunden har ansvar for at datautstyr, programmer og nett til enhver tid tilfredsstiller de krav som stilles av institusjonens bruk av tjenesten. Dette gjelder blant annet at kunden installerer den antivirus- og brannmurprogramvare som følger med datamaskinen eller som leveres av kundens internettleverandør, og at programvaren oppdateres jevnlig. Videre er det gitt retningslinjer for hvilken nettleser og operativsystem som bør benyttes. Det er ingen absolutte regler, men kontoavtalene viser at dette er forhold som vil kunne bli vektlagt dersom det forekommer tap som er forårsaket av at betalingen ikke blir foretatt i henhold til kundens forutsetninger. Slike vurderinger vil også kunne spille inn i forhold til misbruk av kontoen og spørsmålet om kunden har opptrådt grovt uaktsom, se særlig avsnitt 6.3.2 nedenfor.

5.7.3 Bestemmelser i finansavtaleloven

I finansavtalelovens kapittel 2 V er det fastsatt flere bestemmelser som vedrører misbruk av konto. Dette omfatter hovedregelen i lovens § 34 og de særlige reglene som gjelder for betalingskort i § 35. Det er videre gitt regler om lemping av kontohavers ansvar og tilbakeføring av beløp, jf. finansavtaleloven §§ 36 og 37. Disse bestemmelsene er det redegjort for i avsnitt 2.6 foran. I forhold til det materielle innhold og Banklovkommisjonen og departementets merknader til de enkelte bestemmelsene, vises det til denne fremstillingen. *Banklovkommisjonen* har likevel funnet grunn til å drøfte hvordan misbruksreglene har fungert i praksis, med særlig henblikk på de nettbaserte betalingstjenestene.

Hovedregelen i finansavtaleloven innebærer at så lenge kontohaveren ikke har utvist grov uaktsomhet eller forsett, kan ikke kontohaveren holdes ansvarlig for urettmessige belastninger, sml. også avtaleloven §§ 28-31 om ugyldige viljeserklæringer i forhold til svik mv. Lavere grad av uaktsomhet fører således ikke til økonomisk ansvar for kontohaver. Det at en utenforstående legitimerer seg i samsvar med kontoavtalen, vil imidlertid gi et holdepunkt for å hevde at kontohaveren ikke har opptrådt tilstrekkelig aktsomt. Her vil man kunne komme opp i situasjoner hvor kontohaveren hevder at for eksempel PIN-koden har vært betryggende oppbevart, mens institusjonen vil hevde noe annet. Man har imidlertid ikke funnet grunn til å gå så langt som å innføre en særskilt bevisbyrderegel for institusjonen. Det er ellers forutsatt at det må påligge institusjonen å sikre beviset for at vedkommende har legitimert seg i samsvar med avtalen, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 143. Videre er prosessbyrden lagt på institusjonen. Dette innebærer at institusjonen uten videre vil ha plikt til å tilbakeføre beløpet. Institusjonen kan bare fri seg fra denne plikten ved å bringe saken inn for nemnd- eller domstolsbehandling. Dersom saken blir avvist fra nemndbehandling, inntrer plikten til tilbakeføring på ny. I det følgende gjennomgås noen relevante saker fra Bankklagenemnda i forhold til misbruk av nettbanktjenesten. Det vises for øvrig til avsnitt 6.3.2 punkt 2) nedenfor.

I sak BKN-04132 hadde kontohaver, en skole, hatt innbrudd i sine lokaler. Kontohaver opplyste å ha oppbevart en personlig kode og et sikkerhetskort sammen i et låst arkivskap, som ble brutt opp. Skolens konto ble misbrukt for til sammen 23.000 kroner ved overføringer i nettbank. Nemnda antok at misbruket enkelt kunne ha vært forhindret, ved at koden og sikkerhetskortet hadde vært oppbevart atskilt. Nemnda kom til at misbruket var muliggjort ved grov uaktsomhet og at kontohaver kunne holdes ansvarlig, jf. finansavtaleloven § 34.

Bankklagenemnda kom i sak BKN-04098 til samme resultat hvor en menighets nettbankkonto ble misbrukt som følge av innbrudd og tilegnelse av kode og sikkerhetskort som var oppbevart sammen i et pengeskrin.

I BKN-07044 hadde kontohavers datter urettmessig overført 100.000 kroner fra kontohavers brukskonto til sin egen konto via nettbank. Det var etter nemndas oppfatning ikke grunn til å kritisere kontohaver for å ha oppbevart sikkerhetskortet i en skuff i sin stue. Det var heller ikke grunnlag for å kritisere kontohaver for å ha en telefon som har en funksjonalitet der man kan bla i tidligere inntastede siffer. Nemnda fant det klart at kontohaver ikke hadde muliggjort misbruket av kontoen ved grov uaktsomhet, slik banken fremholdt. Kontohaver ble derfor ikke holdt ansvarlig for det tapte beløpet.

I BKN-07150 hadde kontohavers sønn misbrukt kontohavers konto i innklagede bank ved to nettbankoverføringer på til sammen 12.500 kroner til sin konto i en annen bank. Nemnda la til grunn at sønnen måtte ha hatt kjennskap til kontohavers personlige kode, samt hatt kodebrikken. Det var uavklart hvorledes kontohaver hadde oppbevart koden. Nemnda viste imidlertid til at sønnen hadde utvist et forbrytersk forsett, og bedratt sin mor på en utspekulert måte, og kom til at misbruket ikke var muliggjort ved grov uaktsomhet. Banken kunne derfor ikke holde kontohaver ansvarlig for beløpet etter finansavtaleloven § 34.

Ansvaret for kunden er begrenset til disponibelt beløp på kontoen på belastningstidspunktet, jf. finansavtaleloven § 34 annet ledd første punktum. Dette er for øvrig ikke et like relevant tema i forhold til urettmessig belastning av konto i nettbank. Dersom en uvedkommende ved hjelp av kundens brukeridentifikasjon kommer seg inn på vedkommendes nettbankkonto, kan jo denne disponere kontoen som om den var kundens egen konto. For noen banker er det for øvrig nå innført krav om inntasting av engangskode per utført transaksjon. Bankene har videre innført beløpsbegrensninger for overføringer via nettbank, se Bankenes Standardiseringskontors anbefaling nr. 8 og avsnitt 1.3 foran. Slik sett vil misbruket kun beløpe seg til de til enhver tid gjeldende overføringsbegrensninger i vedkommende bank. I visse tilfeller kan imidlertid grensen settes høyere, noe som av og til kun fordrer at man besitter den nødvendige brukerlegitimasjon, se avsnitt 6.2.3 nedenfor.

Begrensningen til disponibelt beløp gjelder for så vidt ikke dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har medvirket forsettlig til at vedkommende kunne legitimere seg, jf. finansavtaleloven § 34 annet ledd siste punktum. Som følge av at disponibelt beløp kan bestemmes av vedkommende som besitter nødvendig brukerlegitimasjon, er imidlertid ikke denne regelen like aktuell.

Når det gjelder betydningen av at kontohaveren varsler om andres urettmessig bruk, vises det til avsnitt 2.6.2 foran.

Del III
Et nytt regelverk

Kapittel 6
Nytt regelverk for nettbasert betalingsoverføring

6.1 Vurdering av reglene for nettbasert betalingsoverføring

6.1.1 Tapssituasjoner som følge av kundens egne feil

Det er foran i avsnitt 5.5 gitt en beskrivelse av gjeldende ansvarsregulering mellom kunden og institusjonen dersom det oppstår utilsiktede eller feilaktige nettbaserte betalingsoverføringer og tapssituasjoner som følge av kundens feilbruk. Som det der fremgår, har ikke finansavtaleloven egne bestemmelser om ansvarsreguleringen når det gjelder slike tilfeller. Reglene i finansavtaleloven § 34 gjelder bare andres misbruk av bankkonto. Oversikten foran tar utgangspunkt i kontoavtalen mellom kunden og institusjonen, samt relevante lovbestemmelser og alminnelige erstatningsregler.

Kontoavtalene bygger i stor grad på gjeldende lovgivning, først og fremst finansavtaleloven, men det er på visse punkter inntatt bestemmelser som konkretiserer forhold som blant annet er fastlagt i rettspraksis. Når det gjelder feiltasting og utilsiktede betalingsoverføringer, er det fastslått at – så lenge kunden har legitimert seg i henhold til kontoavtalen – betalingsoppdragene behandles og gjennomføres i henhold til oppgitt kontonummer uavhengig om det er korrespondanse mellom kontonummer og mottakers navn. Feil registrering er således et forhold som kunden som utgangspunkt står ansvarlig for.

Fra dette utgangspunktet må det gjøres unntak for de tilfeller hvor banken kunne ha oppdaget og unngått konsekvensene av feilen, for eksempel gjennom å varsle kunden om feilen. I slike tilfeller vil banken etter alminnelige erstatningsregler kunne pålegges ansvar, jf. avsnitt 5.5.7 foran.

Heller ikke ehandelsloven gir noe klart svar i forhold til ansvarsforholdet ved egne feil fra kundens side. I ehandelsloven er det for så vidt inntatt regler om feiltasting, men gir ikke et klart svar dersom det faktisk oppstår feiloverføringer. Avtalelovens bestemmelse om feilskrift kan heller ikke anses som et godt grunnlag for å holde institusjonene ansvarlig ved feilbruk, jf. de sikkerhetstiltak og kontrollrutiner som er iverksatt av næringen, se avsnitt 5.5.6 foran.

I betalingssystemloven er det gitt regler som skal sørge for sikker og effektiv betaling. Dette må i prinsippet innebære at institusjonen kan holdes ansvarlig for økonomisk tap som er påført kunden dersom institusjonens betalingssystemer ikke tilfredsstiller de ulike kravene til sikkerheten i betalingssystemet, herunder brukersikkerhet, som loven medfører, jf. for så vidt Justisdepartementets uttalelse i brev til Finansdepartementet av 31. oktober 2006. Kredittilsynet har også fastsatt en forskrift med hjemmel i loven, se avsnitt 5.5.5 foran. Som nevnt er det imidlertid vanskelig å vurdere om feiltasting og annen feilbruk fra kundens side bør fanges opp av institusjonens påkrevde kontrollrutiner. Tiltakene som er iverksatt av næringen selv, er forhold som med styrke vil kunne bli påberopt i denne sammenheng. Etter *Banklovkommisjonens* oppfatning vil det på grunnlag av betalingssystemloven vanskelig kunne statueres et ansvar for institusjonene i tilfelle av feiltasting eller andre brukerfeil fra kundens side med mindre ansvaret kan grunnes på at systemets sikkerhets- eller kontrollmekanismer må anses utilstrekkelig, og burde ha vært utformet slik at de feil det gjelder burde ha vært fanget opp.

I avsnitt 5.5.7 er det redegjort for om en bank med nettbanktjeneste kan holdes ansvarlig etter alminnelige erstatningsregler i situasjoner hvor kunden gjør feil som medfører et økonomisk tap for denne. Når det gjelder spørsmålet om et eventuelt kontrollansvar, er det antatt at institusjonen må pålegges ansvar dersom den ikke har gjort det som var mulig å gjøre for å unngå feilen. Dette er imidlertid et vanskelig vurderingsspørsmål og vil bero på en rekke faktorer. Det nevnes at nettbasert betalingsoverføring utføres via til dels kompliserte og komplekse tekniske og datamessige systemer, og dette medfører at det også foreligger ulike typer av risiko for brukerfeil og misforståelser fra brukerens side, selv om det er usikkert om institusjonen kan pålegges et kontrollansvar dersom det oppstår tap i denne sammenheng. Bankene har nylig satt i verk ytterligere sikringstiltak for å redusere risikoen for brukerfeil, og økt mengden av informa-

sjon om sikkerhets- og kontrollprosedyrer ved bruk av nettbanktjenesten, blant annet også for å påvirke kundene til å opptre med aktsomhet.

I forhold til spørsmålet om banken kan holdes ansvarlig på objektivt grunnlag, vil en rekke momenter inngå i ansvarsvurderingen, herunder prinsipper utviklet over tid i rettspraksis på erstatningsrettens område. Det foreligger imidlertid lite av rettspraksis som vedrører ansvarsforholdene ved nettbaserte betalingsoverføringer eller på nært beslektede områder. Det knytter seg derfor praktisk sett atskillig usikkerhet til hva som må antas å være rettstilstanden generelt og i enkelttilfelle på nettbankområdet.

Banklovkommisjonen mener ut fra dette at kunder i mange tilfeller ikke kan regne med å kunne kreve erstatning fra nettbanken for tap ved utilsiktede og feilaktige betalingsoverføringer som har sammenheng med bruk av feil beløp, kontonummer eller betalingsdag. Regler om objektivt ansvar må i alle tilfelle utformes med atskillig fleksibilitet slik at ansvaret i det enkelte tilfelle kan allokeres på en fornuftig og rimelig måte alt etter de bakenforliggende omstendighetene som forårsaket det aktuelle tapet. Det vises i denne forbindelse særlig til hovedprinsippene for regelsettet som er nedfelt i avsnitt 6.3 flg. nedenfor. Volumet av nettbasert betalingsoverføring har i løpet av få år vist seg å øke meget sterkt, og en meget stor del av bankkunder innenfor privatmarkedet og næringslivsmarkedet gjør regelmessig bruk av nettbaserte betalingstjenester. Finansnæringen antar også at den sterke veksten vil fortsette i de kommende år. Selv om det for tiden ikke foreligger noe tallmateriale eller andre opplysninger om feilfrekvens mv., er det *Banklovkommisjonens* vurdering at det foreligger et klart behov for en avklaring ved lovgivning av ansvarsforholdene ved utilsiktede betalingsoverføringer via nettbaserte betalingssystemer. Det vises også til avsnitt 6.1.3 nedenfor.

6.1.2 Tapssituasjoner som følge av andres misbruk

Foran i avsnitt 5.7 er det gitt en beskrivelse for reglene ved uvedkommendes urettmessige tilgang til og misbruk av konto. Selv om det ble forutsatt at også elektroniske betalingsinstrumenter var omfattet av bestemmelsene i finansavtaleloven § 34, ble det i loven § 35 fastsatt en særskilt ansvarsregulering for andres misbruk av betalingskort. Departementet vurderte for øvrig om det burde trekkes et skille mellom elektroniske betalingsinstrumenter på den ene side og utbetaling med manuell kontroll på den annen side. Banklovkommisjonens opplegg for ansvarsreguleringen ble imidlertid opprettholdt.

Utgangspunktet er slik sett at det i rettslig sammenheng kun skal skilles mellom betalingskortene og de øvrige betalingsinstrumentene. Dette må – i tråd med de teknologiske endringer som har skjedd de siste årene – imidlertid modifiseres noe. Selv om det kun er betalingskort som er unntatt fra den alminnelige reguleringen i finansavtaleloven § 34, taler mye for at reglene i § 34 ble utformet med sikte på de tradisjonelle betalingstjenestene, som for eksempel giro. I denne sammenheng kan det vises til forskriftshjemmelen som ble inntatt i finansavtaleloven § 35 sjette ledd om at bestemmelsen der helt eller delvis kan vedtas å gjelde også for andre typer betalingsinstrumenter. Videre var mange av de elektroniske betalingstjenestene som forelå tidligere, ikke knyttet så tett opp til en brukerlegitimasjon som betalingskortene – og nå de nettbaserte betalingstjenester. *Banklovkommisjonen* viser videre til Banklovkommisjonens uttalelse i Utredning nr. 1 (NOU 1994: 19 Finansavtaler og finansoppdrag) side 110, som er inntatt i avsnitt 2.6.1 foran, hvor det ble antatt at ansvar og risikovurderinger vil kunne bli «nokså ulike for instrumenter utstedt og kontrollert av institusjonen, og for hjelpemidler som betaleren selv eller en tredje part er eier av eller ansvarlig for (telefon, hjemmeterminaler m.v)».

Ut fra de risikobetraktninger som er gjort i forhold til andres misbruk av en kundes konto knyttet til nettbank og/eller telefonbank, fremstår disse nettbaserte betalingsoverføringssystemene som forholdsvis utsatte. Gjeldende ansvarsregulering som fremgår av både kontoavtalen og finansavtaleloven, etterlater også det inntrykk at kundene i flere typetilfeller vil kunne holdes ansvarlig også ved andres misbruk av kundes nettbankkonto(i). I denne forbindelse vises det også til at finansavtalelovens regel om at ansvaret ikke kan overskride belastningsgrenser, jf. lovens § 34 annet ledd annet punktum, ikke er like aktuelt for nettbanktjenesten ettersom dette i stor grad kan styres av den som får tilgang til tjenesten, herunder uvedkommende. Det vises ellers til avsnitt 2.6.2 foran.

Det bør skilles mellom de tilfeller hvor kundens konto misbrukes som følge av urettmessig tilegnelse av kode mv. uten tilknytning til kundens nettkobling og de tilfeller hvor tredjemann urettmessig skaffer seg tilgang til systemet og urettmessig foretar disposisjoner av en kundes konto enten etter å ha vært i ulike former for kontakt med kunden eller via nettverket og/eller oppkobling til kundens datamaskin eller annen nettverkstilkobling.

I de førstnevnte tilfellene vil kunden kunne holdes ansvarlig dersom kode og annen brukerlegitimasjon er oppbevart sammen med informasjon om kontonummer eller annen nødvendig brukerlegitimasjon. Ved uaktsomhetsvurderingen etter finansavtaleloven § 34 kan konklusjonen bli at kunden har utvist grov uaktsomhet i slike tilfeller. Dette er også slått fast i flere saker for Bankklagenemnda, se avsnitt 5.7.3 foran.

Når det gjelder annen urettmessig tilgang fra tredjemanns side, vises det til beskrivelsen av en rekke situasjoner som kan medføre at utenforstående får tilgang til en kundes nettbankkonto(i), se foran avsnitt 5.6.2. Det er særlig angrep på kundens datamaskin som utpeker seg som den største risikofaktoren i forhold til misbruksfaren ved bruk av nettbasert betalingstjeneste. Ut fra bestemmelsen i finansavtaloven § 34 sett i sammenheng med de respektive kontoavtalene, vil kunden i en del tilfeller kunne bli holdt ansvarlig for slike angrep og oppståtte tapssituasjoner. Denne bestemmelsen inneholder således ingen begrensning av kundens ansvar her slik som ved misbruk av betalingskort, jf. finansavtaleloven § 35. Som nevnt foran i avsnitt 5.1 er det imidlertid mye som tyder på at bestemmelsene i finansavtaleloven § 34 hva gjelder ansvarsreguleringer for andre betalingstjenester enn betalingskortene i stor grad var knyttet opp mot de tradisjonelle betalingsinstrumentene som de ulike girotjenestene. I mangel av andre rettslige holdepunkter, er det imidlertid finansavtaleloven § 34 og kontoavtalene, med tilhørende rettspraksis, som er de avgjørende rettskildene ved vurdering av gjeldende rettstilstand. Slik sett vil kunder kunne bli påført store økonomiske tap uten at ansvaret overfor institusjonen vil være begrenset. Etter *Banklovkommisjonens* vurdering er det derfor her behov for å avklare ved lovgivning i hvilken utstrekning en regulering av ansvarsforholdene ved nettbaserte betalingstjenester bør baseres på prinsipper tilsvarende de som ligger til grunn for gjeldende lovregler i finansavtaleloven § 35 om tap som skyldes tredjemanns misbruk av betalingskort, eller i tilfelle utformes ut fra andre utgangspunkter. Det vises for øvrig til avsnitt 6.1.3 nedenfor.

6.1.3 Sammenfatning

Etter *Banklovkommisjonens* oppfatning har betalingstjenester basert på brukerlegitimasjon som inngangskriterium markerte iboende risiki sett fra kundenes side, enten det dreier seg om feilbruk eller misbruk. Det foreligger imidlertid få dokumenterte tilfelle hvor nettbankkunder er påført tap som følge av en utilsiktet betalingsoverføring, og bildet er det samme hva angår uvedkommendes misbruk av nettbankkonti. Det kan likevel ha forekommet tilfelle av utilsiktede eller urettmessige betalingsoverføringer uten at tapet av en eller annen grunn ikke er blitt belastet kontohaveren. Uavhengig av disse forhold må en regne med at det i fremtiden vil kunne oppstå slike tapssituasjoner ved bruk av nettbaserte betalingstjenester uten at det er grunnlag for å anslå omfanget. Risikoen for feilbruk eller misbruk må likevel antas å være reell nok. Nettbaserte betalingstjenester, særlig nettbank og telefonbank, utgjør allerede en meget betydelig del av dagens tilgjengelige betalingsoverføringsordninger, og dens andel i markedet for betalingstjenester må fortsatt antas å øke vesentlig.

Det vises særlig til avsnitt 1.3 foran hvor det fremgår at det på nåværende tidspunkt er ca. 2,8 millioner nettbankkunder i Norge. Det er dessuten antatt at dette tallet vil øke i årene fremover, og det nevnes i denne sammenheng at antall nettbankkunder økte med 300.000 i 2007.[1] Bruken av nettbaserte betalingstjenester vil også påvirkes av omfanget av bankfilialer hvor det er mulig å foreta regningsbetaling. Bruk av filialer knyttes i større grad nå enn tidligere opp mot rådgivning, lån og eiendomsmegling.[2] Det nevnes for øvrig at flere av bankinstitusjonene har lagt til rette for uttak, innskudd, betaling av regninger mv. i eksempelvis dagligvareforretninger, se avsnitt 3.2.1 foran. Bruk av denne tjenesten og dens betydning for fortsatt manuell regningsbetaling er usikker på nåværende tidspunkt. I takt med den økte bruken av Internett, antar *Banklovkommisjonen* uansett at de nettbaserte betalingstjenester vil være den praktisk sett dominerende betalingstjeneste for regningsbetaling i årene fremover. Brukerkretsen vil således utvides, og brukerkollektivet vil omfatte personer med varierende teknisk og datamessig innsikt ut fra de enkeltes personlige forutsetninger. Selv om de nettbaserte betalingstjenestene på nåværende tidspunkt brukes mest av personer i alderen 25-32 år,[3] vil således eldre mennesker – uavhengig av brukernes egne ønskemål – bli en stadig større brukergruppe. Evnen til korrekt bruk, nødvendig innsikt og oversikt over de nettbaserte betalingstjenester må antas å være delvis aldersbestemt.

Ved vurderingen av behovet for en lovregulering av ansvarsforholdene ved bruk av nettbaserte betalingstjenester, mener *Banklovkommisjonen* ut

1 Sparebankforeningens Nettbankundersøkelse 2008.
2 Sparebankforeningens Nettbankundersøkelse 2008.
3 Sparebankforeningens Nettbankundersøkelse 2008.

fra dette at det avgjørende må være at bruk av nettbasert betalingsoverføring, det vil si nettbank og telefonbank, faktisk medfører ulike typer av risiko for at det oppstår tap for en kunde, og at det i lys av den store praktiske og kommersielle betydning av nettbaserte betalingstjenester, er viktig å ha et regelsett på plass som kan håndtere tilfelle av tap som vil kunne ramme den enkelte kunde urimelig hardt. Slike risiki kan imidlertid reduseres ved kontinuerlig utvikling av sikkerhets- og kontrollsystemer, men i hvilken utstrekning dette kan eller vil bli gjort, beror i stor grad også på hvilke virkninger tiltakene generelt sett vil få for brukervennlighet og bruk av nettbaserte betalingstjenester. Det er neppe til å unngå at det til nettbaserte betalingstjenester som er utformet for å kunne håndtere store transaksjonsvolumer, fortsatt vil knytte seg ulike, men typiske risiki, som fra tid til annen vil materialisere seg og føre til tap for så vel bankene som deres kunder.

1) *Banklovkommisjonen* mener at bestemmelsene i finansavtaleloven ikke gir adekvate svar når det gjelder ansvarsreguleringen i forholdet mellom bankinstitusjonen og kunde når det gjelder tap som er utslag enten av kundens brukerfeil eller av andres misbruk av nettbankkonto. Det dreier seg her om tekniske kompliserte systemer som er under stadig utvikling, og som krever omfattende og til dels komplisert brukerveiledning for å motvirke at utilsiktede eller feilaktige betalingsoverføringer finner sted. Det vil således være et mangfold av forskjellige forhold som kundene må forholde seg til og rutinemessig ta i betraktning dersom tap skal unngås. Dette omfatter blant annet inngangsprosedyrer og inntasting av betalingsinformasjon som går utover tradisjonelle betalingsoverføringsformer. At selve overføringene ikke er direkte knyttet opp mot en nærmere bestemt sikkerhetsprosedyre, gjør dessuten at risikoen for kundens egne feil er vesentlig mer fremtredende enn ved bruk av betalingskort. I samsvar med drøftelsen foran legger *Banklovkommisjonen* til grunn at det foreligger et behov for utforming av en ny lovfastsatt ansvarsregulering som gjenspeiler og er tilpasset disse forhold.

Utgangspunktet etter finansavtaleloven er i og for seg at kontohavere fritt kan disponere innestående på sin konto ved blant annet uttak og betalingsoverføringer, jf. finansavtaleloven § 24. Slik sett vil disposisjoner av kunden – enten de er tilsiktede eller utilsiktede – i utgangspunktet måtte anses som gyldige og behandles av banken i henhold til de betalingsinstruksjoner som gis av kunden, jf. også kontoavtalene. Som nevnt i avsnitt 5.1 foran, må det imidlertid antas at reglene i finansavtaleloven, bortsett fra lovens § 35 om misbruk av betalingskort, er utformet først og fremst med sikte på tradisjonelle betalingstjenester og ikke nettbaserte betalingstjenester med den variasjonsbredde og kompleksitet som nå er utviklet av banknæringen. På side 110 i Banklovkommisjonens utredning nr. 1 ble det blant annet fastslått at «ansvar og risikovurderinger [vil] kunne bli nokså ulike for instrumenter utstedt og kontrollert av institusjonen, og for hjelpemidler som betaleren selv eller en tredje part er eier av eller ansvarlig for (telefon, terminaler m.v)». Denne reservasjonen fra *Banklovkommisjonens* side omfatter også de omfattende systemer for nettbaserte betalingstjenester som er blitt utviklet i løpet av den forholdsvis korte periode som er gått siden finansavtaleloven ble vedtatt. Utviklingen har skapt et behov for ansvarsregulering som finansavtaleloven i sin nåværende form ikke var beregnet på å imøtekomme.

Banklovkommisjonen er klar over at det fra banknæringens side blir og fortsatt vil bli nedlagt et betydelig arbeid når det gjelder å etablere systemer for nettbaserte betalingstjenester som har innbygget omfattende sikkerhets- og kontrollordninger. *Banklovkommisjonen* er også klar over at det fra banknæringens side legges stor vekt på utbygging av informasjonsarbeidet overfor kundene når det gjelder bruksmåte og forsiktighetsregler som bør iakttas. I forhold til vanlige nettbankkunder må det imidlertid også tas i betraktning at institusjonenes krav til kundens bruk av betalingstjenesten, som for eksempel krav som gjelder kunders bruk av sin hjemme-pc og mobiltelefon, oppdatering av virusprogrammer mv., likevel ikke er godt nok kjent for eller kan ventes å bli forstått fullt ut av brukere generelt. Sett fra brukernes side fremtrer nettbaserte betalingstjenester derfor som masseproduserte tjenester med typiske risiki for at utilsiktede og feilaktige betalingsoverføringer kan bli gjennomført, og medføre til dels betydelige tap for den enkelte bruker.

Banklovkommisjonen legger til grunn at vanlige brukere av nettbaserte betalingstjenester i forholdsvis liten grad kan påvirke risikonivået i de nettbaserte systemer, og at brukere også praktisk sett vil ha begrensede muligheter til å gardere seg mot at det fra tid til annen vil oppstå tap som følge av utilsiktede, feilaktige eller urettmessige betalingsoverføringer. Vurdert i forhold til nettbaserte betalingstjenesters store betydning i samfunnsøkonomien og det meget store transaksjonsvolumet fremtrer enkeltstående tap generelt sett som en produksjonskostnad for nettbankinstitusjonenes betalingstjenester. Selv om slike tap i første

omgang i utgangspunktet belastes den nettbank det gjelder, vil dette være en produksjonskostnad som egner seg til fordeling – og pulverisering – over brukerkollektivet via gebyrer eller andre økonomiske fordeler oppnådd ved levering av nettbaserte betalingstjenester, i stedet for å måtte bæres av den enkelte bruker som mer eller mindre tilfeldig rammes i det enkelte tilfelle. Den sikkerhet mot tyngende tap som nettbankkundene vil oppnå via et slikt opplegg, vil praktisk sett ikke kunne dekkes på en tilsvarende rasjonell måte via forsikringer tegnet av den enkelte kunde.

Etter *Banklovkommisjonens* vurdering kan imidlertid brukerne gjennom sin handlemåte på forskjellig vis til dels påvirke risikoforholdene. Det er derfor vesentlig at også brukerne gjennom egen handlemåte og så vidt mulig bidrar til å begrense risiko- og tapsnivået. Ansvarsreguleringen bør derfor utformes slik at også brukerne blir oppfordret til dette. Brukere som utviser handlemåter som markert avviker fra den grad av forsiktighet og aktsomhet som med rimelighet kan kreves av brukerkollektivet, må regne med selv å måtte bidra – innen rimelige rammer – til å dekke tap som kan oppstå. Det er en slik tilnærmingsmåte som ligger til grunn for reglene finansavtaleloven §§ 34 flg. om andres misbruk av bankkonti og betalingskort. I forhold til nettbaserte betalingstjenester, gir denne tilnærmingsmåten også et godt utgangspunkt for utformingen av en regulering av ansvarsforholdene når det gjelder så vel tap som er forårsaket av den enkelte brukers egne feil ved bruk av tjenestene som tap som er forårsaket av andres misbruk av tjenesten.

2) *Banklovkommisjonen* viser til at de krav som fra institusjonenes side stilles til kundene, normalt vil fremgå av kontoavtalenes regler og tilgjengelig brukerveiledning om hvilke forhold kundene skal iaktta og også ha ansvar for. Kontoavtalene har imidlertid karakter av tilslutningsavtaler som kundene må akseptere for å benytte seg av systemet. I dette henseende kan det vises til Carsten Smiths forstudie «Om behovet for en banklovkommisjon» fra januar 1989, der det på side 7 sies allment om rettsvernet for finansinstitusjoners kunder:

> «Utgangspunktet og hovedregelen for de vanlige banktjenester i forhold til forbrukere er avtalefrihet ved utformingen av vilkårene for tjenestene. Dette innebærer at vilkårene i stor utstrekning kan fastsettes ensidig i standardformularer fra bankenes og de øvrige finansinstitusjonenes side.»

Risikoen for at det kan forekomme feil må således sees i sammenheng med de avtalevilkårene som kundene må akseptere for å benytte seg av betalingstjenesten. I denne forbindelse kan risikoen for at det oppstår tap som kunden selv må dekke være forholdsvis stor. Carsten Smith uttalte videre – med henblikk på daværende situasjon – at det finnes generelle skranker for de vanlige banktjenester, men at «disse regler ikke sikrer en tilstrekkelig effektiv sivilrettslig beskyttelse av forbrukerne ved finansielle tjenester». På denne bakgrunn fremmet Banklovkommisjonen i sin tid forslag i sin utredning om finansavtaler og finansoppdrag som først og fremst var utformet med henblikk på kunders bruk av de tradisjonelle betalingsinstrumentene, samt de nye former for betalingstjenester som var utviklet i tilknytning til betalingskortene. Som det fremgår av finansavtaleloven §§ 34 flg. var det risikoen for misbruk av bankkonti fra tredjemenns side som det da ble ansett påkrevd å adressere i den nye lovgivningen. Risikoen for at kunden gjør feil, var og er ikke ansett som like stor ved betalingsinstrumenter som giro og betalingskort, noe som for øvrig er lagt til grunn i vurderingen av de gjeldende regler for disse betalingsinstrumentene, se avsnittene 3.5.1 og 4.6 punkt 2) foran.

Det kan i denne sammenheng vises til Banklovkommisjonens uttalelse i sin Utredning nr. 1, på side 67, som fastslo at

> «det er av viktighet – både av hensyn til kortbrukerne og for å opprettholde tilliten til betalingskortsystemene – at sentrale ansvarsfordelingsspørsmål blir fastsatt i lov. Kommisjonen har derfor foreslått lovregler om *ansvar for misbruk av betalingsinstrumenter*».

Etter *Banklovkommisjonens* oppfatning vil denne uttalelsen, samt de andre bemerkninger som ble gjort på dette tidspunktet, jf. særlig avsnitt 2.6.3 foran, også ha aktualitet i forhold til de nettbaserte betalingstjenester som senere er utviklet og som i dagens situasjon har en dominerende stilling i markedet for betalingsoverføringer. Redegjørelsen foran avsnitt 6.1.1, jf. avsnitt 5.4, viser at risikoen for at kunden gjør egne feil er markert og at slike feil kan føre til betydelige tap som det ikke uten videre er klart alltid eller generelt sett bør bæres av kundene selv. Det foreligger derfor behov for en nærmere vurdering og regulering av ansvarsforholdet mellom bankinstitusjon og kunde. På samme måte foreligger det behov for en nærmere vurdering av ansvarsforholdene når det gjelder tap for kunder som skyldes uvedkommendes misbruk av bankkonti via de nettbaserte betalingstjenestene.

Ved utformingen av nye ansvarsregler om slike forhold vil det etter *Banklovkommisjonens* vurdering være naturlig å ta utgangspunkt i de prinsipielle vurderinger som ligger til grunn for finansavtalelovens regulering av ansvarsforholdene når det gjelder tap som oppstår i forbindelse med gjennomføring av betalingsoverføringer og misbruk av betalingstjenesten. Et sentralt synspunkt i forbindelse med utformingen av finansavtalelovens regler om misbruk av bankkonti og betalingskort var at oppståtte tap i hovedsak burde bæres av betalingssystemet slik at tapskostnadene som hovedregel ville bli pulverisert over brukerkollektivet og dekket via brukergebyrene. Ved detaljutformingen av et nytt regelverk kan det imidlertid være behov for å ta hensyn til at risikobildet ved nettbaserte betalingstjenester til dels er et vesentlig annet enn for de hittil vanligste betalingstjenester. Prinsipielt påvirker dette imidlertid ikke behovet for en lovfastsatt ansvarsregulering.

Banklovkommisjonen mener at behovet for regulering av ansvarsforholdene når det gjelder tap som har oppstått ved bruk av nettbasert betalingstjeneste, gjør seg gjeldende både når det gjelder feilbruk fra kundens side og uvedkommendes misbruk av nettbankkonti. Selv om det i utgangspunktet er forskjell på tilfelle av utilsiktet og urettmessig betalingsoverføring, er dette neppe av avgjørende betydning ved utformingen av en ny regulering av ansvarsforholdene. I begge tilfelle kan det dreie seg om tap som kan tilbakeføres til manglende forsiktighet og aktsomhet fra kundens side når det gjelder å overholde den brukerveiledning som er gitt fra nettbankens side både når det gjelder selve bruken av betalingstjenesten og når det gjelder å hindre at uvedkommende får tilgang til kundens brukerlegitimasjon. Uavhengig av hvilken type av feil som måtte være utvist fra kundens side, vil avvik fra brukerveiledningen kunne føre til meget tyngende tap for den enkelte kunde.

Når det gjelder urettmessig bruk fra tredjemanns side, gjelder ansvarsreguleringen i finansavtaleloven bare tilfelle hvor kundens brukerlegitimasjon er benyttet ved betalingsoppdraget. Det at uvedkommende får tilgang til brukerlegitimasjon og urettmessig bruker en kundes bankkonto, kan i flere sammenhenger henføres til feil og uforsiktighet på kundens side, for eksempel ved at kunden ikke har oppbevart kode i henhold til brukerveiledninger og eller andre gjeldende vilkår for bruk av betalingsinstrumentet. Tilsvarende vil det sentrale ved kundens feil i tilfelle av egen feilbruk av den nettbaserte betalingstjenesten ikke være selve den feil som kan konstateres, men først og fremst at kunden har utvist uforsiktighet eller gjort feil når det gjelder å kontrollere at det betalingsoppdrag som er utformet, er slik som tilsiktet. Også i slike tilfelle er således det avgjørende at kunden har utvist manglende aktsomhet og forsiktighet når det gjelder forhold som må iakttas dersom nettbaserte betalingstjenester skal kunne fungere som et effektivt og sikkert system for nasjonale betalingsoverføringer. Det er således lett gjort for en kunde å gjøre en tastefeil eller andre tekniske feil, men den avgjørende feil fra kundens side er i slike tilfelle at feilen ikke er avdekket av kunden ved rimelig kontroll før betalingsoppdraget er sendt. Et hovedspørsmål når det gjelder kravene til nettbankkunders handlemåte som brukere av en nettbasert betalingstjeneste, er derfor hvilken grad av forsiktighet og aktsomhet som må utvises av kunden selv for å forhindre at tap oppstår som følge av egen handlemåte.

Banklovkommisjonen er derfor kommet til at lovreguleringen av ansvarsforholdene ved nettbasert betalingsoverføring bør baseres på tilsvarende prinsipper i begge typetilfellene. En annen sak er at det ved vurderingen av hvilket ansvar kunden selv bør ha fordi kundens handlemåte innebærer en grov tilsidesettelse av kundens egen plikt til å unngå at tap oppstår, vil kunne få betydning for hvilken feil kunden måte ha utvist i det enkelte tilfellet.

Medlemmene Breck, Dalsøren, Dyrhaug, Løfsgaard og Skrede mener at det er vesentlig prinsipiell forskjell mellom misbrukstilfellene, hvor tap oppstår fordi uvedkommende disponerer urettmessig over kontoen, og feilbrukstilfellene, hvor bare kontohaver opptrer (eventuelt supplert av noen nødvendig brukerlegitimasjon er overlatt til). Disse medlemmer har likevel funnet å kunne gi sin tilslutning til forslagene i utredningen, fordi de samlet sett kan sies å tilstrebe en balanse mellom de krav og forventninger som stilles til henholdsvis kundene og banken.

3) *Banklovkommisjonen* legger til grunn at et nytt regelverk for nettbaserte betalingstjenester vil være av vesentlig betydning både for bankinstitusjoner som tilbyr slike tjenester, og de store grupper av brukere som jevnlig gjør bruk av dem. Etter *Banklovkommisjonens* oppfatning vil det derfor være i samsvar med vår rettstradisjon at et slikt regelverk blir gjennomført ved lovgivning.

Banklovkommisjonen nevner at bestemmelsen i finansavtaleloven § 35 sjette ledd som bestemmer at «Kongen kan i forskrift bestemme at reglene i paragrafen her skal gjelde helt eller delvis for andre typer av betalingsinstrumenter», ble innført primært med tanke på «nye elektroniske betalingstjenester som for eksempel «home-banking»», jf.

Banklovkommisjonens uttalelse i sin Utredning nr. 1 side 146. Departementet opprettholdt bestemmelsen og uttalte at den kunne gjøres gjeldende for andre typer betalingsinstrumenter «dersom det i fremtiden skulle vise seg å være andre instrumenter som bør falle inn under den særlige reguleringen [om betalingskort]», jf. Ot.prp. nr. 41 (1998-99) side 43. Ettersom den foreslåtte reguleringen både vedrører utilsiktede og urettmessige transaksjoner, i tillegg til at virkemåten og risikoaspektene ved bruk av nettbaserte betalingstjenester atskiller seg på flere områder fra betalingskortene, har *Banklovkommisjonen* ikke funnet grunn til å utforme et utkast til en forskrift, jf. finansavtaleloven § 35 sjette ledd. De store potensielle tapssituasjonene som kan oppstå for den enkelte kunde, tilsier også at regelsettet bør fremmes i lovs form.

Det utkast til lovregler som er fremlagt av kommisjonen, er derfor utformet som utkast til endringer i finansavtaleloven og som påbygning av de regler om bankkonti som loven allerede inneholder, se kapittel 9 nedenfor.

6.2 Løsningsalternativer

6.2.1 Innledning

I mandatet om sikkerhet ved bruk av nettbank mv. er det forutsatt at Banklovkommisjonen skal vurdere ulike mulige løsninger for en eventuell tapsfordeling mellom kunden og institusjonen dersom det oppstår tap som følge av kundens egne feil. I oppdraget er det skissert tre alternativer som skal vurderes. *Banklovkommisjonen* har ikke funnet grunn til å gå nærmere inn på andre tenkelige tapsfordelingsløsninger.

Det er forutsatt i oppdraget at Banklovkommisjonen skal ta i betraktning de tiltak som finansnæringen selv nå har iverksatt (se avsnitt 1.3 foran), og i hvilken utstrekning det i tillegg er behov for lovregulering av ansvarsforholdene. Som det fremgår foran avsnitt 6.1.3, mener *Banklovkommisjonen* at tiltakene vil ha en klart positiv innvirkning på risikobildet. Til nettbaserte betalingstjenester vil det imidlertid fortsatt knytte seg typiske risiki for at det fra tid til annen kan oppstå tap for kunder som følge av utilsiktede eller urettmessige betalingsoverføringer ved bruk av systemene for nettbaserte betalingstjenester.

Vurderingen av de tre alternativene er gitt i avsnittene 6.2.2-6.2.4. *Banklovkommisjonen* har på bakgrunn av denne gjennomgangen, fremmet forslag til lovregulering basert på det alternativet som etter *Banklovkommisjonens* vurdering vil gi den mest hensiktsmessige ansvarsregulering. I avsnitt 6.2.5 nedenfor sammenfatter Banklovkommisjonen sin vurdering av løsningsalternativene.

Når det gjelder betalingsoverføring til utlandet har ikke *Banklovkommisjonen* vurdert dette opp mot de skisserte løsningsalternativene. Slik betaling forutsetter til dels annen betalingsinformasjon enn betaling innen Norge, og er regulert på en mer inngående måte i den standardiserte kontoavtalen. Det er også vanskeligere å få tilbakeført slike midler dersom de er sendt feil enten utilsiktet eller urettmessig. Flere institusjoner har dessuten lagt opp sin nettbanktjeneste slik at betaling til utlandet er en tjeneste som kunden spesifikt må bestille og knytte opp mot sin nettbank. Disse forholdene medfører at utenlandsbetaling må sees på som en form for betalingsoverføring som bør behandles særskilt. *Banklovkommisjonen* mener for øvrig at norsk regulering på dette området vil kunne gripe inn i rettigheter og plikter til nettbankbrukere utenfor Norge som ikke nødvendigvis vil være i samsvar med nasjonal rett i hjemstaten, eller med regler og praksis når det gjelder internasjonale betalingsoverføringer.

6.2.2 Ansvar for betalingssystemer med manglende sikkerhet eller lignende

Et første alternativ som skal vurderes, er om finansinstitusjoner skal pålegges erstatningsansvar dersom den tilbyr nettbaserte betalingstjenester med manglende eller utilstrekkelige sikkerhets- og kontrollsystemer. I oppdraget side 2 uttales det i tilknytning til dette alternativet at

> «[k]ommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere hvordan en slik eventuell regulering forholder seg til alminnelige erstatningsregler, og på denne bakgrunn vurdere behovet for en lovregulering. Kommisjonen bes vurdere hvordan en eventuell regel om dette kan utformes – særlig om det er hensiktsmessig med en mer skjønnsmessig regel, eller om man bør stille mer konkrete krav til sikkerheten i systemet for betalingsoverføring. Kommisjonen bes om å gjøre rede for hvordan en slik regel vil fungere i praksis.»

Banklovkommisjonen har i oversikten over gjeldende rett konkludert at det knytter seg betydelig usikkerhet til i hvilken utstrekning en bankinstitusjon i enkelttilfelle vil kunne pålegges objektivt ansvar for tap som en bruker påføres ved utilsiktet eller urettmessig betalingsoverføring (se avsnitt 6.1 flg. foran). Det er derfor i alle tilfelle behov for en avklaring av rettstilstanden gjennom

lovgivning dersom reglene om bankinstitusjoners ansvar skal utformes med utgangspunkt i et erstatningsrettslig alternativ. Slike lovregler vil i tilfelle kunne utformes med utgangspunkt i alminnelige rettsregler om leverandørers ansvar for mangler ved de ytelser som tilbys, eller med utgangspunkt i de synspunkter som ligger til grunn for det ulovfestede objektive bedriftsansvar som er utviklet i rettspraksis. I begge tilfelle vil et hovedspørsmål være hvilken grad av systemsikkerhet bankinstitusjonene plikter å etablere gjennom de sikkerhets- og kontrollordninger som iverksettes for de nettbaserte betalingstjenestene, herunder bankinstitusjonens plikter når det gjelder kontinuerlig oppdatering og videreutvikling av slike ordninger.

Vurderingen av hva som til enhver tid vil være et tilfredsstillende sikkerhetsnivå, vil i stor grad bero på hensynet til brukervennlighet og alminnelige kost-/nyttebetraktninger. Det er likevel ikke til hinder for at institusjoner pålegges ansvar for tap som skyldes at sikkerhets- og kontrollordninger og sikkerhetsnivået for tjenesten generelt ikke er i samsvar med hva allmennhet bør kunne forvente. En slik regel vil kunne utformes etter forbilde av definisjonen av sikkerhetsmangel i produktansvarsloven § 2-1 hvor det heter at produsenten plikter «å erstatte skade som hans produkt volder og som skyldes at det ikke byr den sikkerhet som en bruker eller allmennheten med rimelighet kunne vente». *Banklovkommisjonen* antar at det neppe vil være hensiktsmessig å knytte konkrete sikkerhetskrav til en slik ansvarsregel. Slike krav ville måtte baseres på den kunnskap og erfaring en så langt har oppnådd, og vil vanskelig kunne ta hensyn til at nettbaserte betalingstjenester er et område hvor en fortsatt må vente betydelig teknisk og datamessig utvikling.

Sikkerheten ved nettbaserte betalingstjenester beror imidlertid ikke bare på de sikkerhetsordninger som nettbanken som tjenesteleverandør etablererer. Nettbanktjenesten er i stor grad lagt opp til selvstendig bruk fra brukerens side, slik at sikker og feilfri bruk av tjenesten også forutsetter at brukeren utviser aktsomhet og iakttar nettbankens forsiktighetsanvisninger. Det må dessuten skilles mellom den sikkerheten som er etablert i bankinstitusjonens regi, og den sikkerheten som foreligger i kundens egne datasystem. Kan bankene eksempelvis kreve at bruker installerer spesifikke antivirusprogrammer? Selv om dette skulle være mulig, representerer slike krav store utfordringer. Alle antivirusselskaper jobber kontinuerlig med å detektere nye og truende virus. Det eksisterer således et kappløp mellom selskapene og det vil således variere hvilke selskaper som kommer opp med «medisiner» mot spesielle virus. Krav om at kunden installerer et spesifikt antivirusprogram kan således kun representere en tilstrekkelig sikkerhet mot misbruk for en kortvarig periode.

Banklovkommisjonen mener at det for tiden vil by på betydelige problemer å få gjennomført sikkerhets- og kontrollordninger som gir vesentlig høyere grad av sikkerhet mot brukerfeil enn de rutiner ved overføringer gjennom nettbanktjenesten som for tiden er satt i verk. Det kan i og for seg tenkes et opplegg hvor kontonummer kryssjekkes mot betalingsmottagers navn slik at risikoen for utilsiktede betalingstransaksjoner reduseres ytterligere, jf. avsnitt 5.4.1 foran.

Banklovkommisjonen har ikke funnet grunn til å gå nærmere inn på disse forhold, men registrerer at ytterligere krav til sikkerhetsrutiner vil kunne møte betydelig motstand fra banknæringen. Det nevnes for øvrig at betalingstjenestedirektivet inneholder flere bestemmelser om sikkerhet tilknyttet systemer for betalingstjenester, og at arbeidsgruppen som skal utrede gjennomføringen av betalingstjenestedirektivet i norsk rett vil måtte foreta en vurdering om hvorvidt det skal stilles strengere sikkerhetsmessige krav til slike betalingstjenester.

Uavhengig av slike forhold antar *Banklovkommisjonen* at det praktisk sett i alle tilfelle neppe vil være mulig for bankinstitusjonene fullt ut å eliminere ulike typiske risiki for tap som følge av feil ved bruk av nettbaserte betalingstjenester. I lys av den teknologiske utviklingen på dette området er det viktig at ansvarsreguleringen er utformet slik at den også tar hensyn til det dynamiske trusselbildet som betalingsoverføring via Internett og mobiltelefoner representerer. I analogi med de synspunkter som kan begrunne objektivt bedriftsansvar, vil således et naturlig utgangspunkt være at bankinstitusjonene som tilbyr nettbanktjenester pålegges et lovfastsatt objektivt ansvar for tap som skyldes typisk systemrisiko generelt sett.

En praktisk viktig gruppe av feil fra kundens side i forbindelse med betalingsoverføringer gjennom nettbaserte systemer, vil være tastefeil av ulike slag ved utformingen av betalingsoppdraget som blir oversett av kunden under den kontroll som utføres før oppdraget sendes. Etter kontoavtalene vil bankinstitusjonene normalt ikke ha ansvar for tap som skyldes feil, forsinkelser eller problemer i brukernes egne nettverk, driftsstans, andre kommunikasjonsmessige feil, eller lignende forhold. Ut fra alminnelige erstatningsrettslige prinsipper, vil institusjonene videre vanskelig kunne pålegges et objektivt erstatningsansvar uavhengig

av om, og uten unntak for, at tap er forårsaket av forhold helt utenfor institusjonens kontroll.

Banklovkommisjonen mener at en ansvarsregulering basert på en slik erstatningsrettslig tilnærmingsmåte i praksis vil innby til en nærmere vurdering i enkelttilfelle av skillet mellom systemrisiko og de krav som generelt også må stilles til brukernes handlemåte ved bruk av nettbaserte betalingstjenester. En må derfor regne med at det i de enkelte tilfeller lett vil kunne oppstå tvist om årsaksforholdet, det vil si om årsaken til oppstått tap er en systemrisiko eller forhold som må tilskrives brukerens handlemåte. Slike spørsmål vil vanskelig kunne løses på annen måte enn ved tvistebehandling for domstol eller klagenemnd. Slike tvister kan imidlertid neppe avgjøres uten etter en grundig gjennomgang av svært tekniske og avanserte tekniske forhold og sikkerhetsrutiner mv. vedrørende de nettbaserte betalingstjenester. Dette vil kunne kreve betydelige ressurser både for institusjonen og bruker. Silke forhold er dessuten egnet til vesentlig å redusere effektiviteten i en ansvarsregulering basert på en erstatningsrettslig tilnærmingsmåte, særlig på privatkundeområdet.

Ut fra dette er *Banklovkommisjonens* vurdering at en ansvarsregulering basert på en erstatningsrettslig tilnærmingsmåte generelt sett neppe vil virke på en tilfredsstillende og fullgod måte på dette området, jf. også avsnitt 6.2.5 nedenfor.

6.2.3 Tapsbegrensning (egenandel)

Det andre løsningsalternativet som skal vurderes, gjelder spørsmålet om kunden skal ha en begrenset tapsrisiko i form av en egenandel når kundens egne feil ved utførelsen av betalingsoverføringen har ført til tap. Utgangspunktet for dette alternativet er at den bank som tilbyr nettbaserte betalingstjenester normalt må dekke det tap brukeren påføres for så vidt dette overstiger den fastsatte egenandel, og at tap ut over dette vil bli pulverisert som en systemkostnad eller produksjonskostnad for leverandøren av den nettbaserte betalingstjenesten. Dette vil innebære at bankens adgang til å belaste kundens bankkonto vil være tilsvarende begrenset, eller at belastet beløp må tilbakeføres av institusjonen. I mandatet s. 3 uttales det følgende om dette alternativet:

> «Kommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere hva slags dokumentasjon eller bevis som skal kreves for at institusjonen skal måtte foreta en tilbakeføring til kunden. Det skal videre vurderes om institusjonens plikt til å tilbakeføre beløpet skal inntre straks det har skjedd en feil, eller om institusjonen bare skal ha en slik plikt dersom kunden har lidd et tap. Kommisjonen bes vurdere om og i hvilken grad en slik regel innebærer fare for svindel. Kommisjonen bes vurdere hvordan en slik regel kan utformes. I den forbindelse bes kommisjonen særskilt vurdere om regelen kan avgrenses til feil som skyldes eventuell risiko ved systemet for betalingsformidling, eller om regelen også vil måtte omfatte andre feil, for eksempel feil som skyldes at kunden har misoppfattet et kontonummer. Kommisjonen bes i den forbindelse også om å gjøre rede for mulige bevis- og avgrensningsspørsmål som kan oppstå. Kommisjonen skal videre vurdere hva som eventuelt vil være en rimelig fordeling av tapet mellom kunden og institusjonen.»

1) *Banklovkommisjonen* viser til at dette vil være en form for ansvarsregulering som finansavtaleloven allerede gjør bruk av i regleverket om tap som skyldes andres misbruk av betalingskort, se loven § 35 som det er redegjort nærmere for foran avsnitt 2.6.3. Denne bestemmelsen gjelder imidlertid bare tilfelle av urettmessig bruk i tilfelle hvor betalingskortets personlig kode eller annen lignende sikkerhetsprosedyre er brukt. For tilfelle hvor kunden selv har benyttet betalingskortet på en måte som har medført tap, er utgangspunktet at kundens konto belastes med det beløp betalingstransaksjonen gjelder. Den risiko for feil fra kundens side som normalt vil foreligge i slike tilfeller, har ikke sammenheng med selve betalingskortsystemet. I så måte er det en vesentlig forskjell mellom betalingskortsystemer og systemer for nettbaserte betalingsoverføringer.

Risikoen for utilsiktede og feilaktige betalingsoverføringer som skyldes brukerfeil og kundens bruk av nettbaserte systemer er nært knyttet både til systemenes tekniske oppbygging og til utformingen av de sikkerhets- og kontrollordninger som bankinstitusjonen selv har etablert. Det fremgår også foran avsnitt 6.2.2 som *Banklovkommisjonens* vurdering at bankinstitusjonen som hovedregel bør ha ansvar for og bære tap som er utslag av typiske risiki for feil som knytter seg til slike betalingssystemer. Dette gjelder for så vidt uavhengig av om det dreier seg om brukerfeil eller misbruk fra uvedkommende som har skaffet seg tilgang til nødvendig brukerlegitimasjon, se bemerkningene foran avsnitt 6.1.3. Samtidig er det behov for at ansvarsreguleringen utformes slik at kundekollektivet oppfordres til å utvise aktsomhet og iaktta forsiktighetsregler for å gjøre sitt til å begrense risikonivået. Begge disse synspunkter ivaretas etter *Banklovkommisjonens* mening ved en hovedregel

som innebærer at den enkelte kunde selv – innenfor rammen av en fastsatt egenandel – må bære tap som skyldes egne brukerfeil eller at uvedkommende har skaffet seg tilgang til nødvendig brukerlegitimasjon mv.

Banklovkommisjonen ser betydelige fordeler ved en ansvarsregulering basert på et felles grep uten behov for skiller mellom tilfelle hvor utilsiktede og feilaktige betalingsoverføringer har sin bakgrunn i brukerfeil, systemets sikrings- og kontrollordninger, den brukerveiledning som er gjort tilgjengelig, eller misbruk som følge av at uvedkommende har skaffet seg tilgang til nødvendig brukerlegitimasjon. De rettstekniske og praktiske fordeler er klare nok. Materielt sett er det i stor grad ulike forbindelseslinjer mellom de mulige årsaksforhold for tap som kan oppstå i enkelttilfelle. Det kan således være vanskelig å avgjøre om feilbruk har sammenheng med sikkerheten i nettbankenes eller brukerens eget datasystem, eller med tredjemanns påvirkning av bankens og/eller brukerens datasystemer. Disse forhold taler for at det sentrale element i en ansvarsregulering bør være en hovedregel hvoretter brukeren må dekke det tap som oppstår i enkelttilfeller innenfor rammen av en fastsatt egenandel. I særlig tilfelle vil imidlertid en slik regel kunne gi resultater som vil oppleves som urimelige eller for øvrig ha virkninger som anses som uheldige. Det vil således være behov for enkelte modifikasjoner av hovedregelen.

For det første vil det virke urimelig overfor brukere dersom egenandelsansvaret skulle gjelde også i tilfelle hvor det er godtgjort at årsaken til en utilsiktet eller feilaktige betalingsoverføring er sikkerhetsmangel ved nettbanksystemet. Dette vil være tilfelle hvis de sikkerhets- og kontrollordninger som er etablert av bankinstitusjonen, ikke gir det sikkerhetsnivå som allmennheten med rimelighet kan vente. Tilsvarende bør det gjøres unntak fra brukerens egenandelsansvar hvor tapet skyldes at tredjemanns fremgangsmåter er så vidt spesielle at kunden ikke burde pålegges ansvar dersom det oppstår urettmessig bruk av bankkontoen. Det vises til avsnitt lovutkastet § 37b første ledd annet punktum og merknadene til denne bestemmelsen nedenfor.

For det annet bør det omvendt gjøres unntak fra hovedregelen om brukeres egenandelansvar i tilfelle hvor brukeren ved sin handlemåte markert har tilsidesatt de krav til vanlig aktsomhet og forsiktighet som med rimelighet kan stilles til brukerkollektivet av nettbaserte betalingstjenester. Også finansavtaleloven § 34 skiller mellom grov og vanlig uaktsomhet. *Banklovkommisjonen* mener at det generelt sett er vesentlig at nettbaserte betalingstjenester og brukerkollektivet ikke uten videre belastes også med tap som skyldes grove brukerfeil fra enkeltbrukeres side. Ansvarsreguleringen bør derfor utformes slik at det reageres overfor brukere som utviser grov uaktsomhet ved bruken av nettbaserte betalingstjenester. Også alminnelige rettferdsbetraktninger tilsier dette. Det er derfor påkrevd å supplere hovedregelen med en regel som medfører et mer omfattende ansvar i form av en klart høyere egenandel for brukere som har utvist handlemåter som må karakteriseres som grov uaktsomhet. I denne forbindelse nevner *Banklovkommisjonen* at tastefeil i kombinasjon med manglende bruk av systemets innebygde kontrollordninger, etter omstendighetene vil kunne utgjøre en grov uaktsom. Forhold rundt selve tastefeilen og systemets kontrollordninger, både med henblikk på selve det nettbaserte systemet og situasjoner som kunden befinner seg i, kan imidlertid medføre at feilen ikke kan anses som et resultat av grov uaktsom handling. Det vises for øvrig til avsnitt 6.3.2 nedenfor.

Banklovkommisjonen viser til at unntaket knyttet til grovt uaktsomme og/eller forsettlige handlinger også ligger til grunn for ansvarsreguleringen i finansavtaleloven § 35 første og annet ledd. De vurderinger som har dannet utgangspunkt for disse bestemmelser, er generelt akseptert som en rimelig avveining av de kryssende hensyn, med det resultat at brukeransvaret er undergitt en viss begrensning selv i tilfelle av grove brukerfeil som ikke utgjør forsett på kundens side. I forhold til nettbaserte betalingstjenester bør imidlertid et slikt unntak omfatte både tilfelle hvor en brukers egen handlemåte må betegnes som grovt uaktsom, og tilfelle hvor brukeren ved grov uaktsomhet har muliggjort misbruk fra tredjemenns side. Det er bare i tilfelle av tap som er voldt forsettlig eller ved svik fra brukerens side, at brukeren bør kunne holdes ansvarlig uten begrensning.

Ut fra dette er *Banklovkommisjonen* kommet til at en ansvarsregulering basert på prinsippene i finansavtaleloven § 35 bør utgjøre et velegnet utgangspunkt for utformingen av ansvarsreguleringen for tilfelle av brukerfeil og andres misbruk av bakkonto(i) i forbindelse med nettbaserte betalingstjenester. Etter *Banklovkommisjonens* oppfatning vil kombinasjonen av en hovedregel om et egenandelsansvar for brukeren og et unntak med et klart høyere egenandelsansvar for tilfelle av grove brukerfeil, utgjøre en ansvarsregulering som i praksis er velprøvd og generelt akseptert av de ulike partinteresser. *Banklovkommisjonens* vurdering er derfor at denne modellen er et egnet

utgangspunkt for ansvarsreguleringen for bruk av nettbaserte betalingstjenester.

2) *Banklovkommisjonens* vurdering er at brukerens egenandelsansvar for tap ved utilsiktede, feilaktige eller urettmessige betalingsoverføringer som skyldes brukerfeil eller andres misbruk av bankkonti ved nettbaserte betalingstjenester, bør lovfestes slik at egenandelsbeløpene fremgår av loven selv.

I finansavtaleloven § 35 første ledd er egenrisikoen for innehavere av betalingskort som hovedregel begrenset til 800 kroner i tilfelle hvor misbruk av kontoen har sammenheng med at uvedkommende har hatt tilgang til brukerlegitimasjonen. Banklovkommisjonen foreslo med utgangspunkt i dagjeldende kredittkjøpslov § 13 og kontraktspraksis at egenandelen skulle settes til 500 kroner. Departementet viste i Ot.prp. nr. 41 (1998-99) side 43-44 til at kredittkjøpslovens bestemmelse ikke var blitt justert i forhold til fallet i pengeverdien. Departementet mente at det nå ville være riktig å foreta en inflasjonsjustering og mente at beløpet burde settes til 800 kroner, også fordi gjeldende egenandel var lavere enn grensen på 150 euro i EU-kommisjonens rekommandasjon av 24. november 1988 vedrørende betalingssystemer. Samme beløpsgrense er for øvrig benyttet i betalingstjenestedirektivet 2007/44/EF artikkel 61 nr. 1 i forhold til de uautoriserte transaksjonene.

Banklovkommisjonen mener i samsvar med bemerkningene foran at ansvarsreguleringen for nettbaserte betalingstjenester bør utformes som regler felles for tilfelle hvor tap er oppstått som følge av brukerfeil, herunder tastefeil, og uvedkommendes misbruk. For det første bør kunden ha et egenandelsansvar for tap som oppstår i slike tilfelle. Ansvarsbeløpet i betalingstjenestedirektivet er satt til 150 euro, og ansvarsbeløpet foreslås derfor satt til kr. 1.200. Om det i tilfelle også bør føre til endring av ansvarsbeløpet i finansavtaleloven § 35 er et spørsmål som ligger utenfor Banklovkommisjonens oppdrag. For det annet, kunden bør i begge typetilfeller ha et klart høyere egenandelsansvar dersom tapet er oppstått som følge av handlemåte fra kundens side som utgjør grov feil. Også dette egenandelsbeløpet bør gjelde for begge typetilfelle. Kommisjonen foreslår at dette egenandelsbeløpet som i finansavtaleloven § 35 begrenses til 10 ganger den vanlige egenandel, det vil si til kr. 12.000. For det tredje, anvendelsesområdet for det høyere egenandelsansvar bør som hovedregel knyttes til begrepet grov uaktsomhet, jf. finansavtaleloven §§ 34 og 35, likevel slik at kunden alltid bør ha fullt ansvar og dekke tapet i sin helhet i tilfelle hvor tapet er voldt forsettlig av kunden eller kunden har utvist eller medvirket til svik i forhold til institusjonen. Det vises til avsnitt 6.3.3 nedenfor.

3) *Banklovkommisjonen* viser til at medlemsstatene etter fortalen paragraf 34 inntatt i betalingstjenestedirektivet må antas å ha atskillig handlefrihet når det gjelder utforming av ansvarsreguleringen:

> «However, Member States should be able to establish less stringent rules in order to maintain existing levels of consumer protection and promote trust in the safe usage of electronic payment instruments. The fact that different payment instrument involve different risks should be taken into account accordingly promoting issuance of safer instruments. Member States should be allowed to reduce or completely waive the payer's liability except where the payer has acted fraudulently.»

Banklovkommisjonens forslag om en ansvarsgrense på kr. 12.000 for tap som skyldes grov uaktsomhet fra kundens side er i samsvar med dette selv om betalingstjenestedirektivet selv ikke inneholder noen slik regel for tilfelle av grove feil fra kundens side.

Banklovkommisjonen viser også til fortalen paragraf 32 siste punktum hvor det heter: «This Directive should be without prejudice to the payment service providers' responsibility for technical security of their own products.» Som nevnt i fortalen paragraf 34 kan det tas i betraktning at risikoforholdene varierer med betalingstjenestens art, og at det foreligger behov for å fremme utviklingen av sikkerhetsnivået når det gjelder ulike betalingstjenester. Disse forhold må sees i sammenheng med at betalingstjenestedirektivet ikke har særlige regler om brukeres egenandelsansvar for tap som skyldes utilsiktede eller feilaktige betalingsoverføringer som fremtrer som følge av brukerfeil.

Banklovkommisjonen viser til at direktivet artikkel 74 nr. 1 i og for seg kan tyde på at kontohaveren skal bære det fulle ansvar for tap som måtte oppstå i tilfelle hvor det har skjedd en utilsiktet betalingsoverføring som følge av brukerfeil fra kontohaverens side. Det sies der at et betalingsoppdrag som er utført i samsvar med de instruksjoner som institusjonen har mottatt, «shall be deemed to have been executed correctly», det vil si skal anses som korrekt utført av institusjonen. På bakgrunn av fortalens paragrafer 32 og 34 forstår *Banklovkommisjonen* denne bestemmelsen slik at den ikke utgjør en uavbeviselig lovpresumpsjon, og at bestemmelsen derfor ikke er til hinder for ansvar for institusjonen i tilfelle hvor brukerfeilen eller den utilsiktede betalingsoverføringen har sin bakgrunn i at sikkerhets- og veiledningsnivået i den nettbaserte

betalingstjenesten ikke kan anses tilstrekkelig til å forebygge slike forhold. Det vises for så vidt til bemerkningene foran vedrørende forståelsen av direktivets formålsparagrafer 32 og 34.

Banklovkommisjonen mener i samsvar med dette at de bestemmelser om brukeres egenandelsansvar som foreslås, herunder et høyere ansvar ved grove feil, reelt er et uttrykk for prinsippet om at ansvaret for tap som skyldes typiske risiki knyttet til det tekniske opplegg for og sikkerhetsnivået når det gjelder nettbaserte betalingstjenester, i hovedsak bør bæres av nettbankene selv om den lovregulering som foreslås ikke også formelt er basert på en rent erstatningsrettslig tilnærmingsmåte. Generelt sett vil det til nettbaserte betalingstjenester knytte seg risiko for tap for kunder som følge av feil- eller misbruk i større grad enn andre former for betalingsinstrumenter, særlig fordi nettbanktjenester brukes av kunder med ganske forskjellig grad av teknisk innsikt i hvordan systemet fungerer. Videre mener *Banklovkommisjonen* at denne form for ansvarsregulering vil føre til at nettbankene intensiverer sitt utviklingsarbeid for å gjøre nettbaserte betalingstjenester til en rasjonell og sikker form for betalingsoverføring som vil bli møtt med tillit fra brukerkollektivets side, jf. for så vidt fortalen paragraf 32 og 34. Det er for øvrig i vedlegg 1 nedenfor gitt en beskrivelse av innholdet i betalingstjenestedirektivet, og det vises til at betalingstjenestedirektivet for tiden gjennomgås i sin helhet av den arbeidsgruppe som er nedsatt av Finansdepartementet, se foran avsnitt 1.2.

4) Nettbaserte betalingstjenester kan gjelde overføring av beløp av høyst forskjellig størrelse. Risikoen for tap som følge av brukerfeil eller andres misbruk av bankkonto vil således øke med beløpets størrelse i det enkelte tilfellet, og generelt må en regne med at risikoen for store tap er større for nettbank enn for betalingskort. I forhold til brukere flest vil betalingsoverføring av store beløp også stå i en viss særstilling innenfor det totale antall av betalingsoverføringer som den enkelte bruker får utført via nettbaserte betalingstjenester. Dette medfører i seg selv at den enkelte bruker vil ha oppfordring til selv å påse at det ikke skjer brukerfeil som fører til utilsiktede overføringer. Generelt sett innebærer det også at det innefor rammen av en lovfastsatt ansvarsregulering normalt bør kreves at den enkelte bruker utviser en større grad av forsiktighet og aktsomhet for å motvirke egne brukerfeil ved overføringer av betydelig beløp. Det vises til avsnittene 6.3.2 og 6.3.3 nedenfor.

I forhold til risikoen for tap som skyldes andres misbruk av bankkonti er det imidlertid ikke like klar sammenheng mellom tapsrisiko og den enkelte kundes handlemåte. Det vesentlige en bruker kan gjøre for å motvirke andres misbruk, vil være å utvise forsiktighet og treffe tiltak for å forhindre at andre får tilgang til nødvendig brukerlegitimasjon. Her er vi på et område hvor selv beskjeden mangel på aktsomhet fra kundens side kan føre til betydelige tap, og hvor enkeltbrukere i flere tilfeller vanskelig kan innvirke vesentlig på risikoen for misbruk fra tredjemanns side. Tapets størrelse i enkelttilfeller beror generelt sett også på tredjemanns handlemåte.

For å begrense risikoen for store utilsiktede eller urettmessige betalingsoverføringer har nettbankene innarbeidet sikkerhetstiltak i sine nettbaserte systemer i form av beløpsgrense for samlet overføring fra en konto over et fastsatt tidsrom. Nettbankene bruker noe ulike beløpsgrenser, men vanligvis ligger beløpsgrensen på 300.000 kroner for totale overføringer i løpet av en måned, det vil si en beløpsgrense som langt overskrider vanlig beløpsgrense for de fleste betalingskort. Den enkelte kunde gis imidlertid adgang til å få fastsatt en annen – lavere eller høyere – beløpsgrense, enten gjennom nettbanken eller ved personlig kontakt med banken. Det er derfor vanlig at kunden om nødvendig – ved hjelp av sin brukerlegitimasjon – kan få fastsatt en høyere beløpsgrense ved gjennomføringen i enkelttilfelle av en betalingsoverføring som overstiger systemets beløpsgrense. En tredjemann som urettmessig har skaffet seg tilgang til nettbanktjenesten, vil således også i stor grad kunne gjøre det samme.

Banklovkommisjonen mener at brukere generelt må utvise en høyere grad av aktsomhet for å forhindre egne brukerfeil ved gjennomføringen av betalingsoverføringer av beløp av en størrelse som langt overstiger hva som er vanlig for kunden og for brukere flest. Dette bør det tas hensyn til ved vurderingen av om det foreligger grov uaktsomhet på kundens side, jf. avsnitt 6.3.2 punkt 1) nedenfor. Det kan likevel reises spørsmål om ansvaret for en kunde som i slike tilfelle har fremkalt et betydelig tap ved brukerfeil som utgjør grov uaktsomhet, bør kunne pålegges å dekke en større del av det tap som overstiger den ansvarsgrense som er foreslått lagt til grunn ved brukerfeil som utgjør grov uaktsomhet, det vil si 12.000 kroner. Et alternativ vil være å fastsette en særskilt ansvarsgrense for tilfelle hvor betalingsoverføringen overstiger et bestemt beløp. Et annet alternativ vil være å åpne for at en klagenemnd eller domstol i særlige tilfelle kunne pålegge kunden å dekke inntil det dobbelte av ansvarsgrensen. Slike løsninger er imidlertid lite egnet for de tilfeller hvor et stort tap er oppstått som følge av at en tredjemann urettmessig har

skaffet seg adgang til å overføre midler fra kundens konto.

Banklovkommisjonen viser til at en bankinstitusjon ved utformingen av sikkerhetsnivået i sitt nettbaserte betalingstjenestesystem vil kunne fastsette beløpsgrenser som – i samsvar med det som er gjort for betalingskort – vil være romslige i forhold til ordinære betalingsoverføringer for brukere flest. Banken vil også kunne fastsette særskilte fremgangsmåter eller bygge inn særskilte varslingsordninger for tilfelle hvor en kunde vil forhøye den vanlige beløpsgrense, og som derfor gir en høyere grad av sikkerhet mot tap som følge av utilsiktede og utrettmessige betalingsoverføringer. Ut fra dette mener *Banklovkommisjonen* at de beste grunner taler mot å fremme forslag om en særskilt ansvarsgrense for tilfeller hvor kunden har utvist grov uaktsomhet ved gjennomføringen av en betalingsoverføring av uvanlig størrelse. For øvrig vil en slik særlige regel også kunne innebære en ytterligere komplikasjon av ansvarsreguleringen, og dessuten i et begrenset antall tilfeller lett innby til kostnadskrevende tvister mellom institusjonen og enkeltkunder.

Banklovkommisjonen viser til at ansvarsreguleringen for betalingskort i finansavtaleloven som er basert på de samme prinsipper som ligger til grunn for kommisjonens lovutkast, har vist seg å virke på en tilfredsstillende og allment akseptert måte. De tap som er oppstått er i seg selv betydelige, men sett i forhold til de meget store transaksjonsvolumene, tross alt beskjedne og har neppe medført høyere gebyrer for bruk av betalingskort utstedt av norske finansinstitusjoner enn for utenlandske betalingskort. Det er grunn til å anta at det samme vil være tilfellet for nettbaserte betalingstjenester selv om den lovfastsatte ansvarsregulering medfører at tap ved bruk av nettbaserte betalingstjenester i hovedsak vil bli pulverisert over brukerkollektivet og dermed mulig må dekkes via gebyrer for bruk av betalingstjenesten.

En kunde som har utvist eller medvirket til svik ved gjennomføringen av en betalingsoverføring, bør imidlertid alltid kunne holdes fullt ut ansvarlig for det tap som oppstår for nettbanken.

6.2.4 Korrigering av feilbetalingen

Det siste løsningsalternativet omtalt i oppdraget til Banklovkommisjonen gjelder hvorvidt finansinstitusjonen skal gis en rett til selv å korrigere betalingsoverføringer som skyldes kundens egne feil. Det er i denne sammenheng vist til finansavtaleloven § 31 om feil som skyldes institusjonens egne forhold. Dette er en bestemmelse som bare vedrører de tilfeller hvor institusjonen ved en feil har godskrevet uriktig konto eller uriktig beløp, og regelen er at institusjonen kan rette feilen ved å belaste den aktuelle kontoen innen utløpet av tredje virkedag deretter, jf. bestemmelsens første ledd første punktum. Selv om fristen er gått ut, er det forutsatt at institusjonen kan kreve tilbakesøking fra kontohaveren etter alminnelige rettsregler, jf. bestemmelsens fjerde ledd. Det siktes her til de ulovfestede regler om condictio indebiti, jf. Banklovkommisjonens Utredning nr. 1 (NOU 1994:19 Finansavtaler og finansoppdrag) side 141. Det er antatt at kontohaveren i de fleste tilfeller frivillig vil medvirke til tilbakebetalingen. I motsatt fall vil institusjonen i den grad den har rett til å kreve tilbakesøking måtte inndrive kravet på vanlig måte.

I mandatet, på side 3, er følgende uttalt i forhold til det foreslåtte alternativet:

> «Kommisjonen bes vurdere om en slik regulering er hensiktsmessig. Kommisjonen bes vurdere om det bør være tidsmessige begrensninger eller andre former for skranker for institusjonens korreksjonsadgang. Kommisjonen bes videre vurdere hva slags dokumentasjon eller bevis som skal kreves for at banken skal kunne foreta en korreksjon. Kommisjonen bes i den forbindelse vurdere om det er hensiktsmessig at institusjonen ved å foreta en korreksjon, bringes inn i forholdet mellom betaleren og mottakeren, jf. for eksempel en situasjon der betaleren og mottakeren er uenig om beløpets størrelse er korrekt. Kommisjonen bes videre vurdere om og eventuelt i hvilken grad institusjonen løper en risiko dersom den foretar korreksjon på feilaktig grunnlag.»

Banklovkommisjonen har forstått løsningsalternativet dit hen at det vedrører de tilfeller hvor kunden har gjort en feil og hvor institusjonen skal gis en mulighet til å korrigere kundens feilaktige behandling av betalingsoppdraget. Dersom det oppstår et tap, er dette imidlertid et forhold som kunden må svare for. En regel om at institusjonen i slike tilfelle skal holdes ansvarlig dersom den ikke klarer å rette opp i feilen, kan sees på som et utslag av det første løsningsalternativet, jf. avsnitt 6.2.2, og er således utelatt i den videre vurderingen. Drøftelsen er derfor knyttet opp til den tekniske og praktiske muligheten til å korrigere feilbetalingen.

1) *Banklovkommisjonen* er kommet til at det neppe vil være hensiktsmessig å basere en løsning for tilfelle av utilsiktet betalingsoverføring som følge av kundens egen feil, på regler om institusjonens adgang til å korrigere feiloverføringen. Over-

ført på nettbanktjenesten mener *Banklovkommisjonen* at et system med korrigering vil rokke ved de grunnleggende hensyn bak utforming og utvikling av nettbaserte betalingsoverføringsmekanismer, nemlig at betalingstransaksjonene blir utført på en effektiv og rask måte. Etter betalingstjenestedirektivet 2007/64/EF artikkel 69 er det for eksempel bestemt at betalingsoverføringer skal godskrives mottakers konto senest virkedagen etter at overføringen ble utført. Frem til 1. januar 2012 kan imidlertid betaler og institusjonen avtale at godskriving kan skje inntil 3 virkedager etter at betalingsoverføringen fant sted.

Banklovkommisjonen mener at det normalt vil være forbundet med betydelige vanskeligheter å gjennomføre en korrigering i de tilfeller hvor betalingsoverføringen allerede er godskrevet mottakers konto. Det må legges til grunn at mottaker i flere tilfeller vil motsette seg at de innbetalte pengene blir tilbakekalt. En løsning måtte være at kontoavtalene bestemmer at en kunde må akseptere at kreditterte beløp på vedkommendes konto, kan trekkes tilbake dersom betaleren hevder det har skjedd en feil. I så fall vil korrigering likevel forutsette at mottakeren ikke hevder å ha rett til det overførte beløp, noe som reelt vil bety at korrigeringen kan gjennomføres med mottakerens samtykke. I øvrige tilfelle vil nettbanken bli involvert i en tvist mellom betaleren og betalingsmottakeren uten egentlig å ha ansvar for hvordan tvisten skal løses. En lovbestemmelse som vil gi bankinstitusjonen utvidet rett til å foreta tilbakeføring selv etter at betalingen er godskrevet mottakerens konto, og uten mottakers samtykke, vil, slik Justisdepartementet har uttalt i sitt brev til Finansdepartementet av 31. oktober 2006, på side 4, bidra til «å skape en viss usikkerhet i betalingssystemet som sådan, fordi brukerne da ikke i samme grad kan innrette seg i tillit til de overføringer som har skjedd».

En annen løsning måtte være å knytte korreksjonsadgangen opp mot perioden fra transaksjonen iverksettes til den godskrives mottakerens konto. En slik korreksjonsadgang er imidlertid knyttet opp til korte tidsrammer. På nåværende tidspunkt vil betalinger bli godskrevet mottaker forholdsvis raskt.[4] Her må det sees hen til de rutiner som bankinstitusjonene følger i forbindelse med betalingsoppdrag, samt behandlingsrutinene i de sentrale avregningssentralene og oppgjørssystemene.

Bankene som tilbyr nettbanktjenester opererer vanligvis med to frister for prosessering av betalingsoppdrag. Det nevnes at kundenes mulighet til å tilbakekalle oppdraget, i henhold til kontoavtalen, vanligvis må skje dagen før avtalt betalingsdag, jf. avsnitt 5.5.2 foran. For betalingsoppdrag som kunden vil ha iverksatt umiddelbart, men som kunden etter at oppdraget er akseptert, oppdager at er feil, er imidlertid kundens praktiske muligheter til å endre oppdraget begrensede selv om bankenes holdninger varierer en del. I noen nettbanktjenester har ikke kunden noen mulighet til å endre betalingsoppdraget etter at dette er akseptert. For andre nettbanktjenester er denne muligheten imidlertid knyttet opp til når banken sender oppdragene til avregning. Tidspunkt for slike utkjøringsfrister er i flere banker satt til ca. kl. 1200 og 2400 på virkedagene.

Etter at en dekningskontroll er gjennomført, sendes betalingsoppdraget til et system for felles avregning mellom bankene, det vil si Norwegian Interbank Clearing System (NICS). Dette systemet er nå tilrettelagt slik at det er to frister for innlevering av betalingsoppdrag, kl. 1430 og kl. 0530. NICS fungerer som kanal for transaksjons- og informasjonsutveksling mellom bankene og Norges Banks oppgjørssystem (NBO), og leverer samlet grunnlag for det endelige oppgjøret mellom bankene. Etter at NBO har bekreftet, normalt innen henholdsvis kl. 1500 og 0600, at de totale avregningene stemmer, sendes en kvittering til NICS. Deretter gis det en oversikt til bankene om hvilke beløp som skal krediteres og debiteres til de enkelte bankene, forutsatt at de respektive bankene har dekning for masseavregningene. I neste omgang foretar bankene oppdatering av sine kundekonti. Hvor raskt dette blir gjort, varierer naturligvis fra bank til bank og med deres behandlingsrutiner, men kan også variere fra dag til dag alt etter hvor mange transaksjoner som skal registreres ut eller inn. Dersom kreditors konto skal godskrives samme dag, må betalingsoppdraget være lagt inn før kl. 1200 i banken, slik at banken kan foreta dekningskontroll før det sendes videre til NICS.

I forhold til eventuelle tidsmessige skranker, må det legges til grunn at en korrigering av feilbetaling møter flere problemer dersom retting skal skje etter at banken har sendt oppdraget til NICS. Etter at denne fristen er gått ut, vil en eventuell korrigering være et spørsmål bankene i mellom. Dette følger videre av bestemmelser for NICS om at mottatte transaksjoner ikke kan trekkes tilbake av den

[4] For betalingsoverføring til mottaker i samme bank som kunden går dette langt raskere i visse banker, noen ganger umiddelbart og noen ganger på det tidspunkt for utkjøringsfristene i bankene, og korreksjonsadgangen må her anses som enda vanskeligere. Banklovkommisjonen drøfter ikke dette nærmere.

aktuelle bankinstitusjonen, og hensynet til et effektivt betalingstransaksjonssystem har her vært avgjørende. For øvrig finner *Banklovkommisjonen* ikke grunn til å gå nærmere inn på de konkrete bestemmelser for behandling av transaksjoner i NICS.

For å unngå problemene ved tilbakeføring av allerede godskrevne beløp, jf. avsnittet foran, burde en slik korrigering i tilfelle foretas før kreditors bank godskriver kontoen. Etter *Banklovkommisjonens* oppfatning vil dette kreve utvikling av mekanismer bankene imellom som vanskelig vil la seg gjennomføre. Dette gjelder særlig det forhold at bankene har forskjellige rutiner og tidsskjema for kreditering av kundekonti.

Banklovkommisjonen er ut fra dette kommet til at en eventuell korrigeringsmulighet måtte skje før den utilsiktede transaksjonen har nådd NICS. Som beskrivelsen foran viser kan imidlertid dette være forholdsvis korte tidsrom, og det må antas at ikke alle feilbetalinger blir oppdaget umiddelbart. Betalingsoppdrag som legges inn etter kl. 1200 på fredag, blir imidlertid ikke behandlet i NICS før mandag morgen. Her kan det slik sett sies at korrigeringsmuligheten er noe videre, men tatt i betraktning at dette i alle tilfelle bare vil gjelde en del av det totale transaksjonsomfanget, legger imidlertid ikke *Banklovkommisjonen* stor vekt på dette.

Banklovkommisjonen er således av den oppfatning at en ordning basert på korrigering av feilbetaling er lite hensiktsmessig sett fra både bankinstitusjonens og kundekollektivets side. Likevel gjennomgås de øvrige vurderingstemaer som er forutsatt i mandatet for å skape et helhetlig bilde av dette løsningsalternativet.

2) Et annet spørsmål som er aktuelt i forhold til en eventuell korreksjonsadgang, er hva slags dokumentasjon eller bevis som skal kreves for at institusjonen skal kunne foreta en korreksjon. Skal det for eksempel kreves at kunden på et eller annet vis godtgjør at betalingsoppdraget har angitt feil mottaker? Her vil det oppstå vanskelige bevisspørsmål, med mindre et krav om korreksjon av betalingsoppdrag blir ansett som tilstrekkelig. Dette er i samsvar med regelen om tilbakeføring av kontobelastninger ved misbruk fra uvedkommende, jf. finansavtaleloven § 37, men denne regelen må sees i sammenheng med ansvarsreglene i lovens §§ 34 og 35. I § 37 er det imidlertid gitt regler om at tilbakeføring ikke gjelder dersom kontohaver har erkjent ansvar for belastningen eller institusjonen bringer saken inn for nemnd- eller domstolsbehandling innen 4 uker, jf. bestemmelsen annet ledd, se også avsnitt 2.6.5 foran. For feilbetalinger vil dette nødvendigvis forholde seg noe annerledes ettersom feilbetalingen beror på kundens egne feil og ikke på misbruk fra uvedkommende. Forutsetningen for en lovregel på området må således være at feiloverføringen i tilfelle må kunne korrigeres av bankinstitusjonen så snart kunden fremmer krav om dette. Som nevnt i punkt 1) foran må imidlertid dette tidvis skje innenfor snevre tidsrammer.

3) Det neste spørsmålet er hvorvidt det er hensiktsmessig at institusjonen bringes inn i forholdet mellom betaleren og mottakeren, for eksempel i den situasjon hvor betaleren og betalingsmottakeren er uenig om beløpets størrelse er korrekt. *Banklovkommisjonen* mener at en eventuell tvist vedrørende korrigering av en betalingsoverføring vil innebære vanskelige bevisspørsmål og kreve mekanismer og prosedyrer i institusjonen som kan være kostnadskrevende og involvere institusjonen i konflikter som egentlig er denne uvedkommende. En slik ordning vil også kunne medføre at en eventuell tilbakekalling eller opprettholdelse av betalingen av kanskje viktig karakter, blir forsinket og får konsekvenser for betaleren eller mottakeren. Med hensyn til målet om effektive betalingstransaksjoner ved hjelp av Internett, mener *Banklovkommisjonen* at institusjonen ikke bør bringes inn i forholdet mellom betaleren og mottakeren. Det vises også til punkt 1) foran.

4) Et annet spørsmål som oppstår i forhold til et regelsett hvor institusjonen gis en rett til å korrigere feilbetalingen, er om og eventuelt i hvilken grad institusjonen løper en risiko dersom den foretar korreksjon på feilaktig grunnlag. Det kan ikke utelukkes at slike situasjoner oppstår dersom institusjonen ensidig legger til grunn at kravet om tilbakebetaling fra betaleren faktisk er riktig og rettmessig. I denne konteksten kan det forekomme korrigeringer på feilaktig grunnlag og som vil kunne få konsekvenser for mottakeren. Avhengig av alvorligheten av disse konsekvensene bør det legges til grunn at mottaker i første omgang vil fremme krav mot betaleren. Dersom det ikke oppnås noen løsning her, kan mottaker i neste omgang velge å fremme krav mot institusjonen. Dersom dette kravet fører frem, og betaleren for eksempel er konkurs, løper institusjonen helt klart en økonomisk risiko for den opprinnelige korreksjonen av betalingen. *Banklovkommisjonen* finner imidlertid ikke grunn til å gå inn på en nærmere drøftelse av sivilrettslige problemstillinger.

5) *Banklovkommisjonen* har ikke funnet grunn til å vurdere nærmere om et slikt regelsett vil fungere på en hensiktsmessig måte for de tilfeller hvor nettbankkontoen blir misbrukt. I disse situasjonene vil transaksjonen som oftest være vanske-

lig å spore, for eksempel fordi gjerningspersonen har sendt pengene til en konto i utlandet. En korreksjon av betalingen vil således være vanskelig å gjennomføre. De nåværende reguleringer i finansavtaleloven fastslår dessuten at institusjonen skal tilbakeføre det aktuelle beløpet, med mindre kontohaveren har erkjent ansvar for belastningen eller institusjonen har brakt saken inn for en nemnd eller domstol, jf. finansavtaleloven § 37, se også avsnitt 2.6.5 foran. *Banklovkommisjonen* kan ikke se at denne bestemmelsen ikke også bør gjelde for misbruk via nettbankkonto. Det mer interessante spørsmål i denne sammenheng er hvorvidt kunden uavhengig av om han eller hun har utvist grov uaktsomhet kun skal svare for en andel av tapet. Dette er drøftet i avsnitt 6.2.3 og er en løsning som *Banklovkommisjonen* har funnet hensiktsmessig. Den nærmere utformingen av et slikt regelsett er gitt i det avsnittet, samt avsnitt 6.3 flg. nedenfor.

6.2.5 Sammenfatning

Foran har Banklovkommisjonen foretatt en gjennomgang og vurdering av de løsningsalternativer som er skissert i mandatet for sikkerhet ved bruk av nettbank. *Banklovkommisjonen* har vurdert alternativene institusjonens erstatningsansvar for manglende sikkerhet eller lignende og institusjonens rett til å korrigere feilbetalingen som lite hensiktsmessige. For en nærmere begrunnelse for dette synspunktet, vises det til avsnittene 6.2.2 og 6.2.4 foran.

Alternativet om at kunden skal ha en begrenset tapsrisiko (en egenandel) ved utilsiktede eller urettmessige betalingsoverføringer som følge av kundens egne feil eller misbruk fra andre, har *Banklovkommisjonen* imidlertid vurdert som en velbalansert løsning i forholdet mellom kunde og institusjonen. I Justisdepartementets brev til Finansdepartementet av 31. oktober 2006, er det lagt til grunn at en slik løsning vil avhenge av hvorvidt andre former for tiltak reduserer risikoen for feil og hvorvidt disse tiltakene gjennomføres. Som nevnt i avsnitt 1.3 foran er det innført en rekke tiltak i og av næringen selv. *Banklovkommisjonen* er imidlertid av den oppfatning at slike tiltak vil være basert på kost-/nyttebetraktninger, og at en ikke kan vente at slike tiltak vil være tilstrekkelige til å fjerne ulike, men typiske risiki for tap knyttet til nettbaserte betalingstjenester, uavhengig av om det gjelder risikoen for kundens egne feil eller risikoen for andres misbruk. Tap som skyldes utslag av slik risiko bør etter *Banklovkommisjonens* oppfatning ikke bæres av den enkelte kunde som rammes, men som hovedregel dekkes og pulveriseres innenfor systemene for nettbaserte betalingstjenester. I dette perspektiv er alternativet om egenandel klart å foretrekke, og Banklovkommisjonens lovutkast er derfor basert på dette alternativ, jf. 6.3 og kapittel 9 nedenfor.

Løsningsalternativet er i utgangspunktet kun knyttet opp til kundens egne feil. I sin gjennomgang av risikoaspekter ved bruk av nettbaserte betalingsoverføringsmekanismer, har *Banklovkommisjonen* imidlertid sett at risikoen for feil fra kundens side knytter seg både til feil bruk av nettbasert betalingstjeneste, og til feil i forbindelse med oppbevaring av kundens brukerlegitimasjon mv. og slik at tredjemann kan få tilgang til betalingstjenesten og misbruke denne, jf. også avsnitt 6.1.3. En bred regulering av kundens bruk av nettbank og de risikoelementer og eventuelle tapssituasjoner som kan oppstå i denne sammenheng, må også sees på som en fornuftig og veltilpasset løsning ut fra dagens situasjon. Det faktum at bruk av nettbanktjenesten og andre til dels avanserte nettbaserte betalingsoverføringsmekanismer på nåværende tidspunkt skjer i et såpass stort omfang og at den formodentlig vil øke i tiden fremover, gjør det også nødvendig med en løsning som gjør at kunden som hovedregel ikke rammes av tap ved overføringer som er forårsaket av egne feil eller misbruk fra andre eller en kombinasjon av dette. Det er imidlertid behov for særlige regler for tilfelle hvor tap kan tilbakeføres til grov uaktsomhet på kundens side. Hovedprinsippene for en ny ansvarsregulering for nettbaserte betalingstjenester fremgår av avsnittene 6.2.3 og 6.3.

Lovutkastet som Banklovkommisjonen fremlegger er utformet etter modell av ansvarsreguleringen i finansavtaleloven §§ 34 flg., særlig prinsippene i § 35. Ansvarsreguleringen i lovutkastet er felles for tilfelle av utilsiktede og urettmessige betalingsoverføringer, og skiller ikke mellom tilfelle hvor det foreligger feil på kundens side og tilfelle hvor uvedkommende har misbrukt kundens konto. Banklovkommisjonen forutsetter også at det vil være aktuelt å videreføre prinsippene i finansavtaleloven §§ 34 til 37 for nettbaserte betalingstjenester. Det vises til avsnitt 6.3 nedenfor, samt kapittel 9.

6.3 Nærmere utforming av regelverket

6.3.1 Egenandelansvaret

I avsnitt 6.2.3 foran har *Banklovkommisjonen* lagt til grunn at løsningsalternativet om begrenset tapsrisiko for feil fra kundens side uavhengig av feilens

art, må sees på som en hensiktsmessig og balansert løsning. Rettstekniske og praktiske fordeler taler også for et slikt felles grep. Dersom institusjonen som utgangspunkt erkjenner ethvert tap unngås dessuten vanskelige problemstillinger knyttet til både systemansvar og korrigeringsmuligheter, jf. henholdsvis avsnittene 6.2.2 og 6.2.4.

Banklovkommisjonen nevner videre at nettbaserte betalingstjenester inneholder en større risiko for at det oppstår tap som følge av forhold på kundens side enn andre former for betalingsinstrumenter, særlig fordi slike nettbaserte tjenester brukes av kunder med forskjellig grad av teknisk innsikt i hvordan systemet fungerer. En bredere regulering i forhold til kunder av nettbanktjenesten mv. kan derfor også sies å være mer nødvendig enn tilfellet er med betalingskort.

Banklovkommisjonen har derfor sett det som hensiktsmessig at kunden ilegges et objektivt ansvar i form av en selvrisiko for alle overføringer som kan innebære et tap på kundens hånd. Dette vil som ved betalingskortene utvilsomt være med på å opprettholde eller skjerpe kontohaverens aktsomhet, noe som er meget viktig i forhold til bruk av de nettbaserte betalingstjenestene. Som ved reglene for betalingskort er det imidlertid ikke gjort et skille mellom bruk av personlig kode mv. og andre sikkerhetskrav enn koder mv., for eksempel stemme eller fingeravtrykk. Alle former for nødvendig brukerlegitimasjon omfattes av bestemmelsen. De ulike risikofaktorene som knytter seg til selve bruken av slike betalingstjenester, bygger opp om dette.

Banklovkommisjonen mener at egenandelansvaret bør settes til 1.200 kroner, jf. for så vidt betalingstjenestedirektivet 2007/44/EF art. 61 hvor egenandelen for uautoriserte transaksjoner er satt til 150 euro. Dette beløpet atskiller seg heller ikke i stor grad fra den som allerede er vel etablert for betalingskortene, jf. finansavtaleloven § 35. Det vises ellers til avsnitt 6.2.3 punkt 2) foran.

Tapsbegrensningen bør imidlertid forholde seg forskjellig alt etter de konkrete omstendigheter som har medført tapet. Målet må i dette henseende være at reguleringen innebærer en rimelig fordeling av tapet mellom kunden og institusjonen, enten det dreier seg om en utilsiktet eller urettmessig transaksjon. Dette henspeiler seg for det første på de tilfeller hvor de sikkerhets- og kontrollordninger som er etablert av bankinstitusjonen, ikke gir et tilstrekkelig sikkerhetsnivå. Dette vil kunne være tilfelle dersom tredjemann urettmessig disponerer kontohaveres bankkonti uten at nødvendig brukerlegitimasjon er benyttet, typisk ved «direkte» utnyttelse av bankinstitusjonens systemer. I disse situasjonene er det urimelig at brukeren skal kunne holdes ansvarlig for det oppståtte tapet, jf. lovtukastet § 37b første ledd annet punktum og merknader til denne bestemmelsen. Det samme bør gjelde dersom tredjemann går frem på en slik måte at det vil være urimelig om brukeren skal kunne holdes ansvarlig, jf. lovutkastet § 37b første ledd annet punktum i.f.

For det andre har *Banklovkommisjonen* funnet det nødvendig å gjøre unntak fra hovedregelen om brukerens egenandelansvar i tilfelle hvor brukeren ved sin handlemåte markert har tilsidesatt de krav til vanlig aktsomhet og forsiktighet som med rimelighet kan stilles til brukerkollektivet av nettbaserte betalingstjenester. Et ubegrenset ansvar er imidlertid ikke ansett som hensiktsmessig og *Banklovkommisjonen* har, med utgangspunkt i gjeldende regulering i finansavtaleloven, foreslått regler om maksimalansvar i slike situasjoner. Dette er behandlet i avsnitt 6.3.2 nedenfor. Hvor kunden har utvist forsett eller svik tilsier alminnelige prinsipper at kundens ansvar skal være ubegrenset. Dette er det redegjort for nedenfor i avsnitt 6.3.3.

Som følge av lovforslaget med en tapsbegrensning for kunden, har *Banklovkommisjonen* sett det som nødvendig å foreslå en lovregel om regressrett for bankinstitusjonene. Institusjonen som tilbakefører betalingsmidler til kunden bør kunne kreve tilbakebetaling av tredjemann av betalingsmidler som denne urettmessig har mottatt som følge av utilsiktet eller urettmessig bruk av nettbasert betalingstjeneste, jf. lovutkastet § 37b syvende ledd første punktum. I forlengelsen av dette har *Banklovkommisjonen* vurdert det som rimelig at eventuelt tilbakebetalt beløp som overstiger institusjonens tap, skal gå til dekning av kontohaveres egenandel av tapet, jf. lovutkastet § 37b syvende ledd annet punktum.

6.3.2 Egenandelansvaret ved grov uaktsomhet

Å supplere hovedregelen med et unntak som medfører et større ansvar for brukere som har utvist grov uaktsomhet er ansett påkrevd. Det vil virke urimelig dersom en bruker som har utvist en handlemåte som klart markerer et avvik fra vanlig forsvarlig handlemåte ved bruk av nettbasert betalingstjeneste kun skal svare for en liten andel av det oppståtte tapet, enten den grove uaktsomhet har medført en utilsiktet eller urettmessig betalingstransaksjon. Ved avgjørelsen av hvilket ansvar brukeren skal pålegges i tilfelle av grove feil, har *Banklovkommisjonen*, som nevnt i avsnitt 6.3.2

foran, særlig sett hen til finansavtalelovens § 35 annet ledd. *Banklovkommisjonen* har ut i fra dette funnet det hensiktsmessig at brukeren ilegges et høyere egenandelansvar pålydende 12.000 kroner dersom kunden har opptrådt grovt uaktsomt. Egenandelansvaret gjelder bare, som ved regelen om objektivt ansvar beskrevet i avsnitt 6.3.1 foran, dersom nødvendig brukerlegitimasjon er benyttet.

For at en handling eller unnlatelse skal kunne kvalifiseres som grov uaktsom kreves det et markert avvik fra vanlig forsvarlig handlemåte, jf. Banklovkommisjonens uttalelse i Utredning nr. 1 side 144. Denne uttalelsen ble også lagt til grunn i Rt. 2004 side 499 som gjaldt tyveri av et betalingskort. I Rt. 1989 side 1318 og Rt. 1995 side 486 ble også en slik forståelse lagt til grunn.[5] I Banklovkommisjonens Utredning nr. 1 ble det også fastslått at avtaler om betalingskort som regel vil inneholde bestemmelser om bruk og oppbevaring av kort og tilhørende kode. Slike handlings- og adferdsregler ble antatt å ligge i bunn for aktsomhetsvurderingen. Det samme må etter *Banklovkommisjonens* oppfatning gjelde for bruk av nettbank, telefonbank eller lignende nettbaserte betalingsinstrumenter i forhold til kundens behandling av de enkelte betalingsoppdragene. Det tas i denne sammenheng utgangspunkt i avtalen som kunden og institusjonen inngår i forhold til bruk av nettbanktjenesten.

1) I standardavtalen som er utarbeidet av Sparebankforeningen og FNH om vilkår for disponering av konto ved nettbank mv for forbruker, er det ikke inntatt bestemmelser som direkte vedrører feil og tap som er forårsaket av kunden i forbindelse med selve betalingsoppdraget. Av regelen om at beløpet overføres til oppgitt kontonummer kan det imidlertid sies å ligge den konsekvens at feil registrering er et forhold som kunden som utgangspunkt står ansvarlig for. Visse bankinstitusjoner har gitt egne vilkår om betaling via nettbaserte hjelpemidler som presiserer dette. Her er det blant annet bestemt at kunden har ansvar og risiko for tap som skyldes feil registrering, teknisk svikt og lignende frem til betalingsoppdraget er mottatt av institusjonen.

Ettersom *Banklovkommisjonen* er innstilt på å foreslå en regel hvor tap som følge av kundens egne feil, enten dette har medført en utilsiktet eller urettmessig betalingstransaksjon, som hovedregel bare skal være gjenstand for en begrenset egenandel, ser ikke kommisjonen grunn til å legge noe videre vekt på kontoavtalen og dens eventuelle betydning i forhold til vurderingen av om kunden har opptrådt grovt uaktsomt eller ikke.

Spørsmålet blir videre hvilke forhold rundt transaksjonen som skal vurderes og vektlegges for å avgjøre om kunden har opptrådt grovt uaktsomt. Det må her for det første sees hen til de sikkerhetsrutinene som bankinstitusjonene selv har innført, jf. tiltakene for nettbanktjenesten som er angitt i avsnitt 1.3 foran. Slik nettbanktjenesten fungerer i dag er det innbygget flere kontrollmekanismer som skal gjøre tjenesten mer sikker for kunden. Dette vedrører blant annet at tjenesten har kontrollbilde hvor kunden kan se kontonummer, beløp, dato og eventuell KID eller melding til mottaker i en oversiktlig form. I tillegg må kunden aktivt ta stilling til informasjonen i kontrollbildet før betalingen blir iverksatt. I dette ligger en kontrollmulighet som kunden selv i varierende grad vil kunne ta hensyn til.

Det at kunden eventuelt bekrefter betalingsoppdraget vil således være et forhold som kan sees på som et avvik fra vanlig forsvarlig handlemåte. Det er imidlertid ikke like sikkert at alle slike tilfeller skal anses som et «markert avvik», og forholdene rundt selve bekreftelsen og kundens bruk av de tilgjengelige kontrollmekanismer vil være viktige faktorer. Kravet til aktsomhet og forsiktighet vil blant annet måtte anses å øke hvor det dreier seg om større betalingsoppdrag. I slike tilfeller vil det antageligvis være lettere å kunne konstatere et markert avvik enn ved de mindre betalingsoverføringene. *Banklovkommisjonen* nevner videre at bankinstitusjonene nå tilbyr nettbank på mobil (mobilbank, jf. avsnitt 5.2.2). Her er oversiktsbildet betraktelig mindre og danner ikke den samme oversiktsformen som vanlige pc-skjermer gjør. Dersom kunden gjør en feil her må det antas at spørsmålet og vurderingen av om kunden har vist et «markert avvik fra vanlig forsvarlig handlemåte» vil kunne falle noe annerledes ut enn dersom kunden har brukt en pc-skjerm.

Hvilke faktorer som vil være relevante ved vurderingen av om det er utvist grov uaktsomhet av kunden er inntatt i lovforslaget, se utkastet § 37b tredje ledd og merknader til bestemmelsen. Den skal for øvrig ikke anses som en uttømmende angivelse.

2) I forhold til de urettmessige transaksjonene og de feil som kan henføres til kunden i denne sammenheng, er det fastslått flere atferdsregler i kontoavtalen mellom partene som vil være relevante i vurderingen av om kunden har opptrådt grovt

[5] Den ellers vanlige henvisning til Rt. 1970 side. 1235 angående kravet til grov uaktsomhet, er ikke like anvendelig her, ettersom den gjaldt forståelsen av dette uttrykket i en straffebestemmelse, sml. også førstvoterende (flertallets) uttalelse om denne saken i Rt. 2004 side 499.

uaktsomt. I standardavtalen punkt 3, er det blant annet slått fast at

> «[k]ontohaver må påse at uvedkommende ikke får kjennskap til personlig kode eller utstyr for supplerende sikkerhetsprosedyre. Personlig kode skal ikke noteres slik at den kan forstås eller brukes av andre. Ved tap av personlig kode og/eller utstyr for å gjennomføre sikkerhetsprosedyre eller mistanke om at dette er på avveie, skal kontohaver snarest mulig melde fra til banken, enten ved egen funksjon for tjenesten eller pr telefon, telefaks eller e-post slik banken har anvist. Banken vil notere tidspunkt for mottak av meldingen og uten ugrunnet opphold sende kontohaver en skriftlig bekreftelse om at meldingen er mottatt. Banken vil ikke kreve vederlag for slik melding om tap av kode/sikkerhetsprosedyre.»

Standardavtalen angir atferdsregler som først og fremst har betydning i forhold til de tradisjonelle former for urettmessig tilegnelse av tilgangsinformasjon og urettmessig bruk av kundens konto, for eksempel ved innbrudd i bolig og/eller tyveri. For å vurdere om kunden i slike tilfelle skal kunne lastes og videre avgjøre om kunden eventuelt har opptrådt grovt uaktsomhet, har *Banklovkommisjonen* gjennomgått relevant praksis fra domstolene og Bankklagenemnda. Ettersom atferdsreglene ikke atskiller seg i stor grad fra de brukerveiledninger som brukere av betalingskort gis, har *Banklovkommisjonen* også gjennomgått praksis i forbindelse med urettmessig bruk av slike betalingsinstrumenter. Det nevnes for øvrig at praksis i forhold til nettbanktransaksjoner er knyttet opp mot gjeldende finansavtalelov § 34 hvor utvist grov uaktsomhet innebærer at kunden holdes ansvarlig for hele beløpet. Dette kan antas å ha hatt en viss betydning på bedømmelsen av om kunden har utvist grov uaktsomhet eller ikke, for eksempel fordi rettsinstansen har ansett det som urimelig at kunden skal måtte holdes for hele beløpet uten at dette uttrykkelig har fremkommet av premissene for avgjørelsen, jf. for øvrig alminnelige prinsipper for lemping av ansvar.

I BKN 2007-150 ble det ikke statuert grov aktsomhet i forbindelse med misbruk av konto ved nettbanktransaksjoner. Det var kontohavers sønn som hadde misbrukt kontoen. Nemnda la til grunn at sønnen måtte ha hatt kjennskap til kontohavers personlige kode, samt hatt kodebrikken. Det var uavklart hvorledes kontohaver hadde oppbevart koden. Nemnda viste imidlertid til at sønnen hadde utvist et forbrytersk forsett, og bedratt sin mor på en utspekulert måte, og kom til at misbruket ikke var muliggjort ved grov uaktsomhet.

I BKN 2007-044 hadde kontohavers datter urettmessig overført 100.000 kroner fra kontohavers brukskonto til sin egen konto via nettbank. Det var etter nemndas oppfatning ikke grunn til å kritisere kontohaver for å ha oppbevart sikkerhetskortet i en skuff i sin stue. Det var heller ikke grunnlag for å kritisere kontohaver for å ha en telefon som har en funksjonalitet der man kan bla i tidligere inntastede siffer, herunder nødvendige koder for å bruke nettbanken. Nemnda fant det klart at kontohaver ikke hadde muliggjort misbruket av kontoen ved grov uaktsomhet.

I sak BKN-04132 hadde kontohaver, en skole, hatt innbrudd i sine lokaler. Kontohaver opplyste å ha oppbevart en personlig kode og et sikkerhetskort sammen i et låst arkivskap, som ble brutt opp. Skolens konto ble misbrukt for til sammen 23.000 kroner ved overføringer i nettbank. Nemnda antok at misbruket enkelt kunne ha vært forhindret, ved at koden og sikkerhetskortet hadde vært oppbevart atskilt. Nemnda kom til at misbruket var muliggjort ved grov uaktsomhet og at kontohaver kunne holdes ansvarlig, jf. finansavtaleloven § 34.

Bankklagenemnda kom i sak BKN-04098 til samme resultat hvor en menighets nettbankkonto ble misbrukt som følge av innbrudd og tilegnelse av kode og sikkerhetskort som var oppbevart sammen i et pengeskrin.

I BKN-07110 var kortholders betalingskort misbrukt ved minibankuttak for til sammen 20.000 kroner den samme dagen han dro på ferie til Syden, og hvor en ung dame flyttet inn i hans hus for å passe hunden. Nemndas flertall fant det mest sannsynlig at betalingskortet med en lapp med pinkoden hadde vært oppbevart sammen på kortholders hjemmekontor med ukontrollert tilgang for tredjemann, og at misbruket var muliggjort ved grov uaktsomhet. Kortholder ble derfor holdt ansvarlig for egenandelen på 8.000 kroner, jf. finansavtaleloven § 35 annet ledd.

I BKN-07146 var kortholder blitt frastjålet betalingskort under uavklarte omstendigheter. Kortet ble misbrukt ved minibankuttak og varekjøp for 19.544 kroner før kortet ble sperret. Korrekt kode ble tastet på første forsøk. Nemndas flertall fant det mest sannsynlig at koden, eventuelt i dårlig kamuflert form, hadde vært oppbevart og kommet på avveie sammen med kortet, og at misbruket var muliggjort ved grov uaktsomhet. I denne forbindelse ble det lagt vekt på at kortet ikke hadde vært brukt i forkant av misbruket slik at det ikke kunne være snakk om en «kikk-over-skulder-situasjon».

I Rt. 2004 side 499 hadde kortinnehaver under et opphold i Barcelona lagt fra seg sine betalingskort i en låst koffert i en låst leilighet. I samme kof-

fert lå en syvende sans, der kodene til kortene – deriblant et kort som ble misbrukt – var skrevet ned på en kamuflert måte. Spørsmålet var om kortinnehaveren ved grov uaktsomhet hadde muliggjort andres misbruk av betalingskortet. Flertallet kom til at kortinnehaveren kunne bebreides, men at forholdet ikke kunne sies å ha vært grovt uaktsomt. I denne forbindelse finner *Banklovkommisjonen* grunn til å nevne en artikkel av Olav Torvund, publisert i Lov&Data 2003 nr. 75 side 1 med tittel: «Kamuflering av PIN-koder: noen refleksjoner om Borgartings lagmannsretts dom i RG-2002-1273 og senere praksis fra Bankklagenemnda.» Den hovedkonklusjon som trekkes er at det ikke i seg selv er grovt uaktsom å notere koden i en kamuflert form og oppbevare dette notatet sammen med kortet. Men koden må kamufleres på en slik måte at det ikke er nærliggende for andre å anta at dette er PIN-koden til betalingskortet.

Når det gjelder den siste avgjørelsens betydning i forhold til urettmessig bruk av en nettbankkonto, nevner *Banklovkommisjonen* at kamuflering av koder ikke er et like aktuelt tema i denne sammenheng. Bruk av engangskodeverktøy vil redusere betydningen og aktualiteten av dette. Det at personlige passord på en forholdsvis enkel måte kan tilegnes vil imidlertid måtte trekkes inn i vurderingen. Dette gjelder særlig dersom dette skjer i sammenheng med tilegnelse av engangskodeverktøyet. Om de er oppbevart på et sikkert sted vil også spille inn i vurderingen, herunder gjerningspersonens fremgangsmåte for å tilegne seg kodene. Jo mer utspekulert dette gjøres, jo mer må det antas å helle i retning av at kontohaveren ikke har opptrådt grovt uaktsomt.

3) *Banklovkommisjonen* finner videre grunn til å nevne at standardavtalen – i forhold til hvordan kunden skal gå frem for å redusere risikoen for at det oppstår misbruk – kun er et utgangspunkt for institusjonens nærmere regulering og veiledning. I institusjonenes egne vilkår forekommer det derfor visse avvik, og reguleringen er noe mer konkretisert enn standardavtalen. I noen nettbankavtaler er det for eksempel fastslått at kunden selv har ansvar for eget utstyr, slik som programvare, maskinvare, telefon, PC, modem, kommunikasjonsutstyr samt annet tilhørende utstyr. Dette er i noen av nettbankvilkårene utformet slik at kunden har ansvar for at datautstyr, programmer og nett til enhver tid tilfredsstiller de krav som stilles av institusjonens bruk av tjenesten. Dette gjelder blant annet at kunden installerer den antivirus- og brannmurprogramvare som følger med datamaskinen eller som leveres av kundens internettleverandør, og at programvaren oppdateres jevnlig, jf. også avsnitt 5.7.2 foran.

Flere av bankinstitusjonene informerer også kundene sine om at de har et ansvar for å beskytte datamaskinen sin. I noen av vilkårene er det også bestemt at institusjonen ikke er ansvarlig for tap som skyldes «ukorrekt bruk» av kunden. Det er nærliggende å anta at «ukorrekt bruk» også vil kunne omfatte annen feilbruk av kunden, som for eksempel at det ikke er installert tilfredsstillende sikkerhetsprogram på datamaskinen, se foran avsnitt 5.7.2.

I denne sammenheng nevner *Banklovkommisjonen* at urettmessig bruk som følge av tilegnelse av nødvendig brukerlegitimasjon nettopp kan oppstå som følge av tredjemanns tilgang til kundens maskinvare, programvare mv., jf. for så vidt avsnitt 5.6.2 punkt 2) foran. Dette kan karakteriseres som en nettbasert fremgangsmåte for å få tilgang til kundens nettbankkonto. Spørsmålet er i denne sammenheng om kunden skal anses for å ha opptrådt grovt uaktsomt dersom institusjonens regler, oppfordringer eller veiledninger ikke er fulgt. Som ved de tradisjonelle fremgangsmåtene for å tilegne seg nødvendig brukerlegitimasjon, antar *Banklovkommisjonen* at svaret på dette vil variere. *Banklovkommisjonen* understreker imidlertid at en regel om at kunden har ansvar for datamaskinen, programvaren mv. ikke kan forstås dit hen at enhver urettmessig bruk som følge av en slik nettbasert fremgangsmåte innebærer at kunden skal anses for å ha opptrådt uaktsomt. Det ville være å nedlegge en for streng handlingsnorm for kundene. I denne forbindelse vises det til departementets uttalelse om grov uaktsomhet i forhold til betalingskortene i Ot.prp. nr. 41 (1998-99) side 44. Her ble det fastslått at en nemnd eller domstol ikke vil kunne

> «legge til grunn at kunden har opptrådt grovt uaktsomt uten at det foreligger særskilte holdepunkter for dette. At PIN-koden er brukt uten at kunden har noen forklaring på hvordan koden er blitt kjent for uvedkommende, kan ikke være tilstrekkelig til å legge til grunn at kunden har opptrådt grovt uaktsomt og på dette grunnlag ilegge ansvar. Koden kan f.eks ha blitt kjent for uvedkommende ved at misbrukeren, uten at kunden har merket det, har iakttatt kundens inntasting av kode i forbindelse med bruk av kortet.»

Det samme må gjelde i forhold til urettmessig bruk av nettbaserte betalingsoverføringsformer som nettbanktjenesten. Det kan for eksempel tenkes at kunden ikke har blitt oppmerksom på at uvedkommende har installert et program på data-

maskinen til kunden og ut fra dette tilegner seg nødvendige inngangsopplysninger til kundens nettbanktjeneste. Denne risikoen vil ytterligere økes dersom kunden bruker en maskin som ikke er hans eller hennes, for eksempel på hotell eller andre steder hvor det er mulig vederlagsfritt eller mot et vederlag å bruke datamaskiner med oppkobling mot Internett.

Dette tilsier likevel ikke at enhver tilegnelse av nødvendig brukerlegitimasjon ved hjelp av nettbaserte virkemidler skal anses å være unnskyldelig. I visse tilfeller antar *Banklovkommisjonen* at kunden kan sies å ha opptrådt grovt uaktsomt. Dette vil for eksempel gjelde de situasjoner hvor kunden har hatt flere anledninger til å installere autentisk programvare som forhindrer datainnbrudd, særlig dersom kunden har blitt tilbudt slik installasjon av bankinstitusjonen eller institusjonen på en enkel måte har tilrettelagt for slik installering. Et annet moment av betydning vil være hvor enkelt inntrengeren har tilegnet seg inngangsopplysningene. Dersom personlig passord er lagret i et dokument på kundens datamaskin vil gjerningspersonene enkelt kunne tilegne seg denne, noe som bør tillegges vekt i denne sammenheng. Med bruk av engangskodeverktøy, vil kodene imidlertid genereres tilfeldig slik at kunden ikke har mulighet til å notere eller lagre denne informasjonen. Det at inntrengeren på enkelt vis får tak i kundens personlige passord vil imidlertid kunne gjøre resten av prosessen med å komme seg inn på kundens nettbank noe enklere, og bør således inngå som et moment i vurderingen av om kunden har opptrådt grovt uaktsomt eller ikke. *Banklovkommisjonen* har imidlertid ikke ansett det nødvendig å foreslå en regel om at kunden blir ansvarlig på lik måte som om vedkommende hadde opptrådt grovt uaktsomt dersom kunden ikke underretter institusjonen snarest etter at kode eller engangsverktøy er kommet bort. Det vises til avsnitt 6.3.4 nedenfor.

De personlige forutsetningene bør også tillegges vekt, enten det dreier seg om datainnbrudd eller tradisjonelt tyveri eller innbrudd. *Banklovkommisjonen* viser her til RG 2002 side 1273 som vedrørte ansvar ved misbruk av betalingskort. Lagmannsretten uttalte at det ved «avgjørelsen av om en person har handlet grovt uaktsomt må det blant annet legges vekt på vedkommendes personlige evner, egenskaper og forutsetninger». Når det gjelder urettmessig bruk via en kundes oppkobling mot Internett, kan således uaktsomhetsvurderingen falle forskjellig ut alt etter kundens kunnskap til datamaskin og installering av sikkerhetsprogrammer. *Banklovkommisjonen* bemerker her igjen at dette blant annet må knyttes opp til hvor lett tilgjengelig bankinstitusjonen har lagt til rette for slik installering.

Det er ellers begrenset med relevant praksis på dette området, og praksis er i stor grad knyttet opp mot tradisjonelle forbrytelser, jf. punkt 2) foran. Dette betyr imidlertid ikke at risikoen for at det skjer urettmessig bruk av en kundes nettbankkonto ved hjelp av nettbaserte virkemidler er liten, og at det vil oppstå spørsmål om kunden har opptrådt grovt uaktsomt i denne sammenheng eller ikke. I fremtiden vil omfanget antagelig avhenge av det teknologiske forholdet mellom bankinstitusjonenes utvikling av sikkerhetsforordninger og handlingsmønstre til datakriminelle.

Når det gjelder krav til dokumentasjon fra kunden i forbindelse med både utilsiktede og urettmessige transaksjoner, vises det til avsnitt 6.3.6 nedenfor.

6.3.3 Ubegrenset ansvar

Banklovkommisjonen har videre foreslått bestemmelser som i særlige tilfelle pålegger kontohaveren fullt ansvar for tap som skyldes feilbruk eller misbruk av den nettbaserte betalingstjenesten. Dette gjelder for det første de tap som er en følge av feilbruk eller misbruk som må anses voldt ved forsett utvist av brukeren eller noen brukeren har overlatt nødvendig brukerlegitimasjon til. Det er imidlertid viktig å merke seg at forsettet – i samsvar med vanlige skyldprinsipper – må henspeile seg på både selve handlingene og konsekvensen av handlingen. I enkelte tilfeller vil det kunne være tvil om det foreligger forsett fra kundens side eller ikke. *Banklovkommisjonen* har for et praktisk tilfelle forsøkt å løse dette ved å bestemme at ansvarsgrensene ikke gjelder ved feilbruk som følge av at kontohaveren eller noen nødvendig brukerlegitimasjon er overlatt, da betalingsordren ble gitt, bevisst har oversett en særskilt varslingsordning etablert for å hindre slik feilbruk, jf. utkastet § 37b fjerde ledd annet punktum. I forlengelsen av dette, er det behov for å skille mellom de ulike ordinære kontrollordninger som er innebygd i systemet generelt og en særskilt varslingsordning, for eksempel et enkelt og særlig iøynefallende kontrollbilde, som aktiviseres i de tilfeller hvor transaksjonen etter beløp eller annen måte atskiller seg fra transaksjoner flest. Da må det kreves at kontohaveren på nytt forvisser seg om at betalingsoppdraget er utformet i samsvar med hans ønskemål før det sendes. Hvis derimot kontohaveren bevisst har oversett en slik tydelig fremkommet kontrollvarsel og likevel sendt et betalingsoppdrag, må det

normalt legges til grunn at kunden må ha tatt risikoen for tap som vil oppstå.

Når det gjelder tap som oppstår som følge av urettmessig bruk, antar *Banklovkommisjonen* at tapet normalt må anses voldt forsettlig dersom kunden har overlatt brukerlegitimasjonen til et familiemedlem som i betydelig grad har belastet kontoen eller belastet den ut over den grensen kontohaveren har fastsatt. I slike tilfeller kan for øvrig fullmaktsbetraktninger føre til samme resultat. I tilfelle hvor en tredjemann har tilegnet seg nødvendig brukerlegitimasjon og misbrukt kontoen, vil forholdet sjelden være at kunden bevisst har utvist en så høy grad av uforsiktighet ved oppbevaringen av den nødvendige brukerlegitimasjonen at tapet kan sies å være voldt ved forsettlig handlemåte fra kundens side. En annen sak er at kunden vil kunne få ansvar for å ha unnlatt å underrette institusjonen etter å ha fått kjennskap til at det har skjedd feilbruk eller misbruk av sin egen nettbaserte konto, se nedenfor avsnitt 6.3.4.

Kan kunden bebreides for å ha oppbevart kode og annet sikkerhetsverktøy skjødesløst og forholdsvis lett tilgjengelig for uvedkommende, vil således kundens handlemåte normalt måtte karakteriseres som grov uaktsomhet i forhold til tap som oppstår som følge av urettmessig bruk. For de nettbaserte fremgangsmåtene, det vil si tilegnelse av nødvendig brukerlegitimasjon ved kontakt med kunden eller kundens datamaskin og programvare via Internett, vil det samme kunne legges til grunn selv om kunden i og for seg har mottatt et varsel via media eller fra institusjonen, om at det må vises særlig varsomhet i forhold til å besøke spesifikke nettsteder, installering av konkrete programmer på kundens datamaskiner eller lignende, men ikke har fulgt opp slike advarsler.

Videre har *Banklovkommisjonen* også gjort unntak for egenandelansvaret i de tilfeller hvor kunden har utvist eller medvirket til svik, jf. henvisningen til finansavtaleloven § 34 fjerde ledd i lovutkastet § 37b femte ledd. Situasjoner med forsett og svik kan for øvrig ha glidende overganger. *Banklovkommisjonen* har imidlertid ikke funnet grunn til å gå nærmere inn på dette, ettersom kunden uansett vil holdes ansvarlig for det oppståtte tapet. Svik vil for øvrig forutsette et avtalt samarbeid mellom kontohaveren og den tredjemann som innehar den konto som betalingsmidlene er overført til. Identiteten til betalingsmottakeren vil imidlertid være kjent som følge av at regelverket mot «hvitvasking» av penger krever at opprettelse av konto bare kan skje dersom innehaveren fremviser pass eller annen sikker legitimasjon (lov av 20. juni 2003 nr. 41 om tiltak mot hvitvasking av utbytte fra straffbare handlinger). I forhold til risikoen for at pengene overføres til utlandet understreker *Banklovkommisjonen* at det gjelder særskilte regler som skal forhindre urettmessige grenseoverskridende transaksjoner. Dersom betalingsmottakeren urettmessig disponerer midler overført til sin konto, vil det normalt innebære overtredelse av sentrale strafferettsbestemmelser som skal motvirke økonomisk kriminalitet. *Banklovkommisjonen* er i og for seg klar over at man ikke kan se bort fra at svik etter samarbeid mellom en kontohaver og en betalingsmottaker også vil kunne forekomme ved nettbaserte betalingstjenester, men en antar at oppdagelsesrisikoen er så vidt påtagelig at dette vil bidra til å redusere omfanget av slik økonomisk kriminalitet. Det vises for øvrig til at det ikke foreligger opplysninger om i hvilken utstrekning det må antas at kunder har eller kan ha utvist svik ved bruk av nettbaserte betalingstjenester.

6.3.4 Underretning til institusjonen

Underretning til institusjonen kan ha viktige økonomiske konsekvenser for kunden i forskjellige tilfelle. Dette henspeiler seg for det første på underretning til institusjonen dersom kunden oppdager forhold som skaper særlig stor fare for misbruk, for eksempel dersom kode eller annet nødvendig tilgangsverktøy kan ha blitt tilgjengelig for uvedkommende. Dersom kunden varsler institusjonen om slike forhold, er *Banklovkommisjonen* av den oppfatning at kunden ikke kan holdes ansvarlig for urettmessige transaksjoner som oppstår i etterkant av slikt varsel. I lovforslaget er det vist til finansavtaleloven § 34 tredje ledd første punktum hvor denne bestemmelsen er inntatt, og *Banklovkommisjonen* viser ellers til kommisjonens Utredning nr. 1 side 143.

For det andre – og motsvaret til regelen foran – bør manglende varsel dersom kunden har fått kjennskap til at nødvendig brukerlegitimasjon er kommet bort eller må ha kommet på avveie, eller innen rimelig tid etter at dette burde være oppdaget, ha visse konsekvenser for kunden. *Banklovkommisjonen* understreker at det er den brukerlegitimasjon som er nødvendig for å få tilgang til tjenesten som må ha kommet bort. Dette omfatter både personlig kode og annen nødvendig sikkerhetsverktøy. Det kan hevdes at kravet om underretning bør gjelde både dersom personlig kode eller annet sikkerhetsverktøy er kommet bort eller på avveie. Det kan her vises til finansavtaleloven § 35 annet ledd bokstav b) hvor kun betalingskort er omtalt og ikke PIN-kode mv., se også Banklovkommisjonens Utredning nr. 1 side 145. Forskjellen

mellom betalingskort og annen nettbasert betalingstjeneste er imidlertid at betalingskortet i seg selv ofte kan lede til urettmessig bruk. Dette gjelder særlig for kredittkortene hvor belastninger kan gjøres ved hjelp av underskrift og ikke inntasting av personlig kode. *Banklovkommisjonen* nevner for øvrig at personlig kode til annen nettbasert betalingstjeneste må antas å kunne gjøre den videre prosessen enklere. Ettersom den ikke alene kan medføre direkte urettmessige betalingstransaksjoner har *Banklovkommisjonen* kommet til at kravet om underretning bare gjelder dersom den nødvendige brukerlegitimasjonen, det vil si personlig kode og annet sikkerhetsverktøy, er kommet bort.

I tråd med betalingskortreglene i finansavtaleloven har imidlertid ikke *Banklovkommisjonen* funnet grunn til å ilegge kunden et ubegrenset ansvar for slike tilfelle, men at kontohaveren i stedet svarer med en begrenset andel satt til 12.000 kroner for den urettmessige transaksjonen, jf. utkastet § 37b annet ledd annet punktum. Banklovkommisjonen bemerker at det ikke stilles krav til grov uaktsomhet etter denne regelen, kun vanlig uaktsomhet. Bestemmelsen pålegger kunden plikt til å foreta en viss kontroll og reagere snarest mulig når tapet av kode mv. er eller burde vært oppdaget.

For det tredje har *Banklovkommisjonen* funnet grunn til å innta en bestemmelse om at ansvarsgrensene ikke gjelder dersom kunden har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til feilbruk eller misbruk av den nettbaserte betalingstjenesten, jf. lovutkastet § 37b femte ledd annet punktum. I en slik situasjon fremstår det som urimelig at korthaveren skal være beskyttet av beløpsgrensen.

6.3.5 Lemping av ansvar

Banklovkommisjonen mener videre at det bør innføres en regel om lemping av ansvar for kunden dersom ansvaret etter forholdene vil virke urimelig tyngende for kunden. Regelen bygger på finansavtaleloven § 36, jf. utkastet § 37c, men er mer rettet mot konsekvensen av at kunden blir pålagt ansvar. Det skal tas hensyn til om måten kontoen kan disponeres på ikke er betryggende, og om den nettbaserte betalingstjenesten er i samsvar med forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner for den nettbaserte betalingstjenesten. Dette bør imidlertid bare gjelde dersom den utilsiktede eller urettmessige betalingsoverføringen har sammenheng med slike forhold.

Det bør også tas hensyn til manglende aktsomhet eller andre forhold på institusjonens side som har medvirket til at den urettmessige eller utilsiktede betalingsoverføringen ble utført. Ved vurdering av om kundens ansvar skal reduseres eller falle bort vil det videre ofte være naturlig å trekke inn kundens forhold. Dersom kontohaveren har opptrådt sterkt klanderverdig vil det kunne være grunn til å ikke redusere kontohaverens ansvar.

For øvrig bør det tas hensyn til praksis i tilknytning til lemping av erstatningsansvar etter skadeserstatningsloven av 13. juni 1969 nr. 26 § 5-2.

6.3.6 Reklamasjon. Tilbakeføring

1) Spørsmålet om institusjonens plikt til å tilbakeføre beløpet skal inntre straks det har skjedd en feil, eller om institusjonen bare skal ha en slik plikt dersom kunden har lidd et tap, er forutsatt vurdert opp mot løsningsalternativet om tapsbegrensning for kunden, jf. mandatet og avsnitt 6.2.3 foran. Det at kunden skal ha lidt et tap forutsetter, i forhold til de tilfelle hvor kunden på utilsiktet vis har gjennomført en betalingstransaksjon, at mottaker av pengene ikke vil eller kan tilbakebetale det urettmessig mottatte beløpet. I forhold til urettmessig bruk av den nettbaserte betalingstjenesten, vil tapet som oftest oppstå umiddelbart, ettersom misbruket er et resultat av en kriminell atferd med et målrettet ønske om gevinst for gjerningspersonen.

Når det gjelder de tilfelle hvor det har forekommet urettmessig bruk, har *Banklovkommisjonen* sett det som hensiktsmessig å videreføre de regler og prinsipper som gjelder for reklamasjon og tilbakeføring ved misbruk av konto og betalingskort, jf. finansavtaleloven § 37. Det vises her til Banklovkommisjonens Utredning nr. 1 side 146-147 og Ot.prp. nr. 41 (1998-99) side 44-45. Deler av de synspunkt og begrunnelser som har fremkommet her, vil også måtte antas å gjelde i forhold til reklamasjon og tilbakeføring ved tap som har oppstått som følge av en utilsiktet nettbasert betalingsoverføring. Utover dette mener *Banklovkommisjonen* imidlertid at prinsippene bør påbygges noe, særlig spørsmål om krav til dokumentasjon fra kunden, jf. lovutkastet § 37d annet ledd.

2) Det at mottaker ikke kan eller vil betale tilbake kan ha sitt utspring i forskjellige faktorer. Mottaker kan for eksempel ha brukt opp pengene uten mulighet til å tilbakebetale beløpet, for eksempel ved konkurs uten at boet gir dekning for det urettmessige beløpet. Det kan også forekomme tilfeller hvor mottaker mener seg berettiget til pengene. Kunden må i verste fall fremme saken for forliksrådet eller domstolene for å få en rettskraftig avgjørelse som kan gjennomføres av

namsmyndighetene. Før pengene kommer tilbake til kunden, kan det slik sett gå lang tid.

Etter *Banklovkommisjonens* mening er institusjonen bedre rustet til å foreta en slik inndriving. Både prosessbyrden som eventuelt legges på kunden og tidsrommet før pengene tilbakebetales, taler for at institusjonens plikt til å tilbakeføre beløpet bør inntre straks. Dette synspunktet bør imidlertid modifiseres noe. Det må antas at det i de fleste tilfelle vil stilles spørsmål ved om kunden har opptrådt grovt uaktsomt, slik at kunden eventuelt bare vil motta en del av det tapte beløpet. Dokumentasjonen om forholdene rundt tapssituasjonen er derfor meget viktig i et økonomisk perspektiv, både for kundens og institusjonens del. Dette spørsmålet var også oppe i forbindelse med forslaget til regler om betalingskortene i finansavtaleloven. Her kom departementet til at en særskilt bevisbyrderegel hvor institusjonen måtte bevise de faktiske forhold rundt den urettmessige bruken, ikke burde forfølges, jf. også avsnitt 2.6.5 foran. Begrunnelsen for dette var at det i praksis vil være kontohaveren som har best kjennskap til de faktiske forhold, blant annet hvordan PIN-koden har vært oppbevart, jf. Ot.prp. nr. 41 (1998-99) side 43 følgende. Det ble ikke antatt å være rimelig at institusjonen skulle pålegges en bevisbyrde for slike forhold.

Overført på de nettbaserte betalingstjenestene, er *Banklovkommisjonen* av den oppfatning at lignende synspunkter bør legges til grunn også her. *Banklovkommisjonen* har imidlertid tatt hensyn til de potensielle sviksituasjonene som kan oppstå ved en slik regulering. For at institusjonen på enklere vis kan vurdere om kunden har gått frem på en måte som kan anses som enten unnskyldelig, grov uaktsom eller forsettlig, mener *Banklovkommisjonen* at reklamasjonen bør begrunne kravet på en rimelig måte. I dette ligger et krav om at kunden gir en beskrivelse av omstendighetene rundt feiltransaksjonen. Kunden plikter i tillegg å gi opplysninger til institusjonen om, og på hvilken måte, det er gjort forsøk på å få betalingsmottakeren til å tilbakeføre beløp som utilsiktet eller urettmessig er overført til mottakeren. Ut fra en slik reklamasjon vil institusjonen ha et bedre vurderingsgrunnlag i forhold til om saken bør bringes inn for nemnd- eller domstolsbehandling, jf. prinsippet om at institusjonen skal ha prosessbyrden i lovutkastet § 37d tredje og fjerde ledd, jf. også finansavtaleloven § 37 annet og tredje ledd.

Om kunden skal bære en større del av tapet eller – for forsetts- og sviktilfellene – fullt ut, avhenger av hva slags avgjørelse kunden oppnår i en nemnd eller domstol. *Banklovkommisjonen* nevner at det på samme vis som ved urettmessig bruk bør foreligge særskilte holdepunkter for at kunden eventuelt har opptrådt grovt uaktsomt eller forsettlig i sin behandling av betalingsoppdraget eller i sin oppbevaring av kode og annet sikkerhetsverktøy og generell håndtering av systemene for de nettbaserte betalingstjenestene. Omstendighetene rundt den utilsiktede eller urettmessige transaksjonen kan – utover reklamasjonen fra kunden – være vanskelig å bevise, noe som bør undergis vanlige parts- og vitneforklaringer med nemndens eller domstolens egen vurdering av forklaringens troverdighet og vekt. Det vises for øvrig til avsnittene 6.3.2 og 6.3.3 foran.

Kapittel 7
Administrative og økonomiske konsekvenser

7.1 Innledning

I denne utredningen fremmer *Banklovkommisjonen* utkast til endringer i finansavtalelovens kapittel 2. Endringene inntas som et nytt avsnitt Va i kapitlet. Utkastet gir kontohavere en større sikkerhet i forhold til potensielle tapssituasjoner ved bruk av nettbasert betalingstjeneste og er ansett som et nødvendig tiltak i forhold til den utvikling som har skjedd innenfor banknæringen og økt bruk av nye og mer avanserte betalingsoverføringsmekanismer.

Lovutkastet viderefører prinsippene fra finansavtalelovens kapittel 2 V, men omfatter, i tillegg til tapssituasjoner som er forårsaket av urettmessig bruk, også de tilfeller hvor det har oppstått tap som følge av utilsiktede betalingsoverføringer. *Banklovkommisjonen* mener at behovet for regulering av ansvarsforholdene når det gjelder tap som har oppstått ved bruk av nettbasert betalingstjeneste, gjør seg gjeldende både når det gjelder feilbruk fra kundens side og uvedkommendes misbruk av nettbankkonti. Selv om det i utgangspunktet er forskjell på tilfelle av utilsiktet og urettmessig betalingsoverføring, er dette neppe av avgjørende betydning ved utformingen av en ny regulering av ansvarsforholdene. I begge tilfelle kan det dreie seg om tap som kan tilbakeføres til manglende forsiktighet og aktsomhet fra kundens side når det gjelder å overholde den brukerveiledning som er gitt fra nettbankens side både når det gjelder selve bruken av betalingstjenesten og når det gjelder å hindre at uvedkommende får tilgang til kundens brukerlegitimasjon. Uavhengig av hvilken type av feil som måtte være utvist fra kundens side, vil avvik fra brukerveiledningen kunne føre til meget tyngende tap for den enkelte kunde.

Banklovkommisjonen har ansett betalingskortreglene som velfungerende i dagens samfunn og har bygget på flere av de momenter som ble lagt til grunn den gang Banklovkommisjonen fremmet forslag om slike regler, jf. Banklovkommisjonens Utredning nr. 1. Utkastet innebærer således i flere tilfeller en tapsbegrensning for kunden dersom det oppstår urettmessige eller utilsiktede betalingsoverføringer.

Banklovkommisjonen har ikke ansett en lovregulering med tilsyn, samt tiltak fra institusjonene selv som tilstrekkelig i forhold til risikoen for at tap som er foranlediget av forhold på kundens side kan forekomme. De elektroniske systemer for betalingstjenester stiller andre krav til kontroll- og sikkerhetsrutiner enn de tradisjonelle papirbaserte tjenestene. Dataene i betalingssystemene representerer videre store verdier. Dette gjør betalingssystemene utsatt for misbruk av systemene, for eksempel urettmessige overføringer eller uttak fra konti, eller organisert sabotasje.

7.2 Økonomiske og administrative konsekvenser for det offentlige

Banklovkommisjonen har ved utarbeidelsen av forslaget om lovregler for nettbasert betalingstjeneste lagt vekt på å utarbeide et så enkelt og videreførbart regelverk som mulig. Dette skulle redusere behovet for det offentlige til å sette seg inn i lovverket.

Banklovkommisjonen anser at den gjeldende forskriftshjemmelen i finansavtaleloven § 35 siste ledd, vil miste noe av sin aktualitet. *Banklovkommisjonen* har likevel ansett det hensiktsmessig å bevare denne hjemmelen. Med den teknologiske utviklingen kan det ikke utelukkes at det etableres nye former for betalingsformidling som bygger på brukerlegitimasjon, men som ikke nødvendigvis er knyttet opp til Internett eller annet elektronisk nettverk.

Ettersom bankinstitusjonene kan forhindre tilbakeføring ved å bringe saken inn for nemnd- eller domstolsbehandling, kan det ikke utelukkes at det jevnt over vil fremmes mange saker for de aktuelle instansene. Det må legges til grunn at flere tvister ikke har kommet så langt under de nåværende reglene, ettersom dette i mange tilfeller har måttet bero på at kunden selv fremmer saken. Når prosessbyrden legges på institusjonen, må det antas at flere saker vil bringes inn. Dette vil særlig angå spørsmålet om kunden har opptrådt grovt uaktsomt eller ikke. *Banklovkommisjonen* antar imidlertid at disse spørsmålene ikke vil by på merar-

beid for instansene. Spørsmål om grov uaktsomhet har allerede i stor grad vært et spørsmål i forhold til særlig betalingskortreglene og instansene må antas å ha mye å bygge på herfra. Mengden av saker vil muligens øke i en periode ettersom praksis tilknyttet nettbaserte betalingsoverføringer og betydningen av grov uaktsomhet opp mot et maksimalansvar for kunden er nytt. Etter en tid vil det imidlertid antas at vurderingene vil bygge på tidligere praksis og institusjonene vil formodentlig i standardtilfeller ikke se noen grunn til å bringe saken inn for nemnd- eller domstolsbehandling.

7.3 Økonomiske og administrative konsekvenser for private

7.3.1 Konsekvenser for kundene

En gjennomføring av utkastet knyttet til urettmessige og utilsiktede betalingsoverføringer via nettbaserte betalingstjenester, vil innebære en økt trygghet og et ytterligere forbrukervern for kundene. Dette må anses som særlig viktig tatt i betraktning den store andelen av den norske befolkning som har tatt i bruk slike nettbaserte betalingstjenester. Store deler av arbeidsoppgavene i forbindelse med betalingsoverføringene er flyttet over på den enkelte kunden og risikoen for at det oppstår urettmessige og utilsiktede transaksjoner har således økt. Håndtering av pengestrømmene er slik sett i stor grad overført til kundene selv. Ansvarsreguleringen tar hensyn til dette på en rimelig måte.

Det er videre mye som tyder på at bruksomfanget av de nettbaserte betalingstjenestene vil øke i tiden fremover. I denne sammenheng er det viktig at brukerne av nettbasert betalingstjenester har tillit til at systemet fungerer på en slik måte at potensielle tapssituasjoner elimineres eller i hvert fall reduseres for kundenes del. Det er ikke bare i kundens interesse at nettbaserte betalingstjenester benyttes av store deler av befolkningen. For institusjonene innebærer slike systemer sparte utgifter i forhold til etablering og drift av filialer.

Under dagens regelverk risikerer kunden å bli utsatt for større økonomiske tap i sin bruk av nettbaserte betalingstjenester. Målet er imidlertid ikke å fjerne enhver risiko ved slik betalingsformidling. Lovutkastet gjenspeiler risikoen tilknyttet slike betalingsoverføringsmekanismer i den forstand at ansvarsgrensen for tap ved urettmessige eller utilsiktede transaksjoner i tilfelle av grov uaktsomhet er satt til et beløp som i forhold til vanlige kunder vil måtte betraktes som forholdsvis høyt. Dette må antas å gi kundene en foranledning til å opptre enda mer varsomt og årvåkent, noe som må antas å være et viktig grep ut fra den store og økende bruken av slike betalingstjenester.

7.3.2 Konsekvenser for institusjonene

Lovforslaget innebærer at institusjonene vil bli pålagt et – i de fleste tilfeller – delvis økonomisk ansvar for tap ved transaksjoner som på utilsiktet eller urettmessig vis er gjennomført som følge av at kunden har gått frem på en feil måte. Forutsetningen er at institusjonen vil ta hensyn til dette som en produksjonskostnad ved utformingen av sitt nettbaserte betalingstjenestetilbud. Det vises til avsnitt 6.1.3 foran.

Det at institusjonene i flere tilfelle kun kan holde kundene ansvarlig for en egenandel dersom det oppstår tap ved nettbasert betalingsoverføring, må antas ha flere konsekvenser for institusjonene. For det første er det mulig at institusjonene utarbeider nærmere retningslinjer for kundens bruk av nettbanktjenesten, både i forhold til oppbevaring av koder, installering av sikker programvare, samt behandling av de enkelte betalingsoppdrag. I forhold til urettmessig bruk kan det med tiden ikke utelukkes at installering av tilfredsstillende antivirusprogramvare og brannmur, er en forutsetning for at kunden skal kunne ha tilgang til betalingstjenestene.

Lovutkastet vil således kunne innebære merarbeid for institusjonene, i hvert fall i en overgangsperiode. Økt tiltak fra institusjonens side kan imidlertid medføre at nettbanktjenesten ikke vil være like attraktiv som tidligere. Her kommer også avveiningen mellom brukervennlighet og sikkerhet inn. Med hensyn til den konkurransesituasjon som eksisterer i banknæringen, må det likevel antas at denne avveiningen faller ut på en slik måte at kundene fortsatt ser fordelen med nettbaserte betalingstjenester samtidig som systemene blir sikrere både i forhold til at det oppstår utilsiktede og urettmessige betalingsoverføringer.

Det tapsvolumet som kan oppstå på institusjonens hånd kan i visse tilfeller være betydelig. Tapet må imidlertid sees i sammenheng med de fordeler institusjonen oppnår ved å tilby disse tjenestene. Merkostnadene vil dessuten kunne innkreves og dekkes gjennom nettbankstjenestens vederlagsordninger eller ved at rasjonaliseringsgevinstene ved å ha etablert slike nettbaserte tjenester blir mindre.

Kapittel 8
Merknader til de enkelte bestemmelser

Banklovkommisjonens forslag til regler for nettbasert betalingsoverføring er foreslått inntatt som et eget avsnitt Va i kapittel 2 i finansavtaleloven. Lovutkastet er slik sett ikke ment å innebære noen endringer av gjeldende regler i loven. Tatt i betraktning viktigheten av dette regelsettet for de enkelte kundene, har *Banklovkommisjonen* ansett det som hensiktsmessig å foreslå reglene i lovs form, jf. også avsnitt 6.1.3 foran. Ettersom mange av momentene i regelforslaget er videreført fra gjeldende regler i finansavtaleloven, særlig reglene for misbruk av betalingskort, er merknadene til visse av bestemmelsene knyttet opp til forarbeidene til disse allerede gjeldende reglene.

Til endringer i lov 25. juni 1999 nr. 46 om finansavtaler og finansoppdrag:

Til § 34. Misbruk av konto m.v.

I *femte ledd annet punktum* er det på samme vis som ved henvisningen til at ansvar ved misbruk av betalingskort er regulert i § 35, inntatt en henvisning til at ansvar ved utilsiktet eller urettmessig betalingsoverføring ved bruk av annen nettbasert betalingstjeneste er regulert i § 37a til § 37d. *Banklovkommisjonen* benytter uttrykket «annen nettbasert betalingsoverføring», ettersom betalingskort også kan sies å være en form for nettbasert betalingsoverføring. Henvisningen medfører at reglene i avsnitt Va ikke gjelder for betalingskortene.

Til kapittel 2 Va. Utilsiktet og urettmessig bruk av ordninger for nettbasert betalingsoverføring

Banklovkommisjonen foreslår et nytt avsnitt Va som vedrører utilsiktet og urettmessig bruk av ordninger for nettbasert betalingsoverføring. Avsnitt V vedrører kun andres misbruk av konto, og *Banklovkommisjonen* har derfor funnet det mer hensiktsmessig at bestemmelsene ikke plasseres her, selv om lovforslaget i stor grad viderefører prinsippene i avsnitt V. Det ville medført en del lovtekniske og materielle endringer i tillegg til at *Banklovkommisjonen* har vurdert at bestemmelsene i avsnitt V har fungert på en tilfredsstillende måte slik de fremstår i dag.

Til § 37a. Virkeområde

I *første ledd* er det fastslått at bestemmelsene i avsnitt Va gjelder betalingsoverføring ved bruk av nettbaserte betalingstjenester. Det vises til finansavtaleloven § 12 første ledd bokstav a) hvor betalingsoppdrag er definert som oppdrag om uttak eller overføring av betalingsmidler. Det er for øvrig markert at bestemmelsene ikke gjelder for betalingsoverføring ved bruk av betalingskort. Det vises til merknadene til § 34 femte ledd annet punktum foran.

I *annet ledd* er det gitt en nærmere definisjon av hva som menes med nettbasert betalingsoverføring. Slik overføring skal forstås som overføring av betalingsmidler fra innskuddskonto i henhold til betalingsoppdrag sendt til, og mottatt av, institusjonen gjennom Internett eller annet elektronisk nettverk. Det vises for øvrig til finansavtaleloven § 9 første ledd om virkeområde for kapitlet. En nærmere definisjon av «betalingsmidler» er videre gitt i finansavtaleloven § 12 første ledd bokstav b). Etter denne bestemmelsen omfatter betalingsmidler blant annet innskudd og kreditt på konto i en finansinstitusjon eller en lignende institusjon som kan disponeres ved bruk av betalingsinstrumenter, herunder nettbaserte betalingstjenester, jf. bestemmelsens bokstav c).

I *tredje ledd* er det bestemt at nettbasert betalingstjeneste skal forstås som ordning for nettbasert betalingsoverføring i henhold til avtale mellom kontohaveren og institusjonen. Nettbank- og telefonbanktjenester er inntatt som eksempler på slike tjenester. På nåværende tidspunkt er det nettopp nettbank og telefonbank som brukes mest av norske bankkunder. Disse tjenestene er koblet opp mot henholdsvis Internett og telefonnettet, og begge fanges opp av definisjonen i annet ledd. Med formuleringen «annet elektronisk nettverk» er formålet at også andre og fremtidige betalingstjenester som er knyttet opp til et nettverk, skal omfattes av bestemmelsene. Bestemmelsene er således ment å kunne følge den teknologiske utviklingen

uten at den skal være begrenset til de nåværende mest brukte nettbaserte betalingstjenestene.

Fjerde ledd første punktum fastslår at bestemmelsene i §§ 37b til 37d ikke kan fravikes ved avtale til skade for kontohaveren. Hovedregelen er dermed at bestemmelsene ikke kan fravikes uavhengig av om kontohaveren skal anses å være en forbruker eller ikke. Etter *annet punktum* er det imidlertid bestemt at dersom en institusjon som tilbyr nettbasert betalingstjeneste, også har etablert en særskilt nettbasert betalingstjeneste bare for næringslivskunder, kan bestemmelsene i §§ 37b til 37d alltid fravikes i avtalen mellom institusjonen og kontohaveren om tilgang til slik særskilt betalingstjeneste uavhengig av om kontohaveren i det enkelte tilfelle opptrer som forbruker eller i næringsvirksomhet. Etter hovedregelen i finansavtaleloven § 2 om ufravikelighet, må det i det enkelte tilfelle avgjøres om kontohaveren har handlet ut fra formål som hovedsakelig ikke er knyttet til næringsvirksomhet. Dette kan imidlertid skape uklare avgrensningsspørsmål i forhold til de nettbaserte betalingstjenestene, fordi enkeltpersoner kan opptre dels som forbruker og dels som næringsdrivende ved bruk av slike betalingstjenester. Bestemmelsen i fjerde ledd annet punktum klargjør at vedkommende alltid anses å opptre i næringsvirksomhet ved bruk av en særskilt nettbasert betalingstjeneste bare for næringsdrivende.

Til § 37b. Utilsiktet og urettmessig bruk av nettbasert betalingstjeneste

Bestemmelsen fastslår spesialregler for nettbasert betalingsoverføring som ikke er betalingskort. På nåværende tidspunkt er det særlig nettbank og telefonbank som utpeker seg. På samme vis som ved betalingskortreglene har *Banklovkommisjonen* sett det som nødvendig at bestemmelsen ikke kun er begrenset til vedkommende som har inngått avtale om nettbasert betalingstjeneste. Ansvarsreglene gjelder både i forhold til kontohaveren, men også andre som vedkommende kontohaver har gitt tilgangsrett til, jf. ordene «noen som nødvendig brukerlegitimasjon er overlatt til». I tillegg gjelder reglene i forhold til handlemåten til andre som kontohaveren har overlatt den nødvendige brukerlegitimasjon til.

I *første ledd første punktum* foreslår *Banklovkommisjonen* at kontohaveren skal ha et objektivt ansvar i form av en selvrisiko begrenset oppad til en egenandel på 1.200 kroner for tap som følge av utilsiktet eller urettmessig betalingsoverføring ved feilbruk eller misbruk av nettbasert betalingstjeneste. Forutsetningen for slikt ansvar er at personlig kode og annen lignende sikkerhetsprosedyre eller sikkerhetsverktøy er brukt for å få utført et betalingsoppdrag. Dette omfatter alle former for nødvendig brukerlegitimasjon for å kunne benytte seg av den nettbaserte betalingstjenesten. Det kan for eksempel ikke utelukkes at nettbaserte betalingstjenester med tiden knyttes opp mot andre sikkerhetskrav enn koder mv., for eksempel stemme eller fingeravtrykk. De ulike risikofaktorene som knytter seg til selve bruken av slike betalingstjenester, tilsier at det ikke bør foretas et skille her.

Dersom nødvendig brukerlegitimasjon er benyttet må imidlertid kunden, uavhengig av om denne er å bebreide, dekke tap opp til 1.200 kroner. Motstykket til dette er at kontohaveren, utover denne egenandelen, ikke kommer i ansvar, med mindre noen av unntakene i bestemmelsene kommer til anvendelse. Det vises for øvrig til avsnitt 6.3.1 foran.

I *annet punktum* er det for det første bestemt at kontohaveren likevel ikke svarer for slik egenandel dersom tapet skyldes at institusjonen ikke byr den sikkerhet mot feilbruk eller misbruk som en bruker eller allmennheten med rimelighet kunne vente. Regelen er utformet etter modell av produktansvarsloven av 23. desember 1988 nr. 104 § 2-1. Det sentrale innholdet er at vurderingen er frigjort fra en vurdering av institusjonens forhold. Det kan således foreligge en sikkerhetsmangel selv om institusjonen har gjort hva man med rimelighet kan forlange av institusjonen. Kriteriene refererer seg til forventningene hos den typiske bruker av produktet og hos det alminnelige publikum som utsettes for den risiko produktet frambyr. *Banklovkommisjonen* viser ellers til Ot.prp. nr. 48 (1987-1988) side 125 flg. Det bør avgjøres konkret om banken i en gitt situasjon kunne ha oppdaget og avverget feilen. Her må det legges vekt på om bankens system tilfredsstiller de krav det er naturlig å stille ut fra foreliggende kunnskap på tidspunktet hvor den utilsiktede eller urettmessige betalingsoverføringen ble gjennomført. Bestemmelsen vil kunne omfatte de tilfeller hvor det har forekommet urettmessig bruk uten at nødvendig brukerlegitimasjon er benyttet, for eksempel dersom tredjemann «direkte» utnytter bankinstitusjonens systemer og urettmessig disponerer kontohaveres bankkonti.

Videre er det bestemt at kontohaveren ikke svarer for egenandelen på 1.200 kroner dersom tapet skyldes at en tredjemann ved inntrenging i elektronisk nettverk, grov tvang eller lignende handlemåte urettmessig har skaffet seg tilgang til nødvendig brukerlegitimasjon eller endret det

betalingsoppdrag kontohaveren har gitt. Bestemmelsen gjør et unntak fra første punktum ved at kunden i visse tilfeller ikke kan holdes ansvarlig selv om nødvendig brukerlegitimasjon er brukt. Det omfatter både de tradisjonelle urettmessige fremgangsmåtene til å tilegne seg nødvendig brukerlegitimasjon som de nettbaserte fremgangsmåtene, i tillegg til andre avanserte former for misbruk av en kundes nettbaserte betalingstjeneste. Det vises til avsnitt 5.6.2 foran. I slike tilfeller har *Banklovkommisjonen* funnet det urimelig at kunden skal kunne holdes ansvarlig. Dersom den urettmessige tilegnelsen av nødvendig brukerlegitimasjon har oppstått som følge av grov uaktsomhet, vil imidlertid kunden måtte svare for en større egenandel.

Bestemmelsen i *annet ledd* setter et tak for kontohaverens ansvar for tap som følge av utilsiktede eller urettmessige betalingsoverføringer ved feilbruk eller misbruk av nettbasert betalingstjeneste. Som ved bestemmelsen i første ledd omfatter dette bare de tilfeller hvor nødvendig brukerlegitimasjon er benyttet.

Etter *annet ledd første punktum* er egenandelansvaret utvidet dersom betalingsoverføringen er gjort mulig ved grov uaktsomhet av kontohaveren, eller av noen som nødvendig brukerlegitimasjon er overlatt til. Egenandelansvaret er i disse tilfellene satt til 12.000 kroner. Det vises for øvrig til avsnitt 6.3.2 foran.

Etter *annet ledd annet punktum* utvides egenandelansvaret tilsvarende dersom misbruk er muliggjort fordi kontohaveren eller noen nødvendig brukerlegitimasjonen er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at brukerlegitimasjonen er kommet bort eller må ha kommet på avveie, eller innen rimelig tid etter at dette burde være oppdaget. Det vises til avsnitt 6.3.4 foran.

Viktige momenter av om det foreligger grov uaktsomhet er nærmere omtalt i bestemmelsens *tredje ledd.* Det skal for øvrig ikke anses som en uttømmende angivelse. Her er det bestemt at det ved avgjørelsen om betalingsoverføringen er gjort mulig ved grov uaktsomhet som nevnt i annet ledd, skal det blant annet legges vekt på om slike krav til forsiktighet og egenkontroll som med rimelighet kan stilles til brukere av nettbasert betalingstjenester, er blitt klart tilsidesatt. Hvordan kunden har gått frem i oppbevaring av koder og i behandling av de enkelte betalingsoppdrag er viktige momenter i en vurdering av om kunden har opptrådt grovt uaktsomt. Som bestemmelsen viser vil krav til forsiktighet og egenkontroll kunne variere fra kunde til kunde. Det er derfor viktig å vurdere kundens kunnskap og innsikt i den enkelte betalingstjeneste. *Banklovkommisjonen* nevner at et viktig moment i denne vurderingen vil være hvordan selve tjenesten er utformet, herunder utformingen og tilretteleggingen av kontrollmekanismer for kunden. Videre vil det være av betydning hvilken veiledning og hjelp institusjonen gir kunden for å hindre at det oppstår tap, og på hvilken måte kunden på dette grunnlag har søkt å sette seg inn i den aktuelle betalingstjenesten.

Videre er det bestemt at det skal legges vekt på i hvilken utstrekning den nettbaserte betalingstjenesten gir slik sikkerhet mot feilbruk og misbruk som en bruker eller allmennheten med rimelighet kunne vente. Vurderingskriteriet må sees i sammenheng med første ledd annet punktum. I de tilfelle hvor tapet skyldes sikkerhetsmangel i tjenestene, vil institusjonen måtte holdes ansvarlig. Poenget etter tredje ledd er at dersom manglende sikkerhet ut fra de krav brukeren eller allmennheten med rimelighet kunne vente, kan sies å være en av faktorene til at tapet har oppstått, vil dette ha betydning i forhold til avgjørelsen av om kunden har opptrådt grovt uaktsomt eller ikke. Det vises for øvrig til avsnitt 6.3.2 foran.

Etter *fjerde ledd første punktum* er det bestemt at ansvarsbegrensningen etter første og annet ledd ikke gjelder tap som er oppstått ved feilbruk eller misbruk av den nettbaserte betalingstjenesten, og som er forsettlig voldt av kontohaveren eller noen nødvendig brukerlegitimasjon er overlatt til. Det vises til avsnitt 6.3.3 foran. Ved forsett bærer kontohaveren som hovedregel hele risikoen for den urettmessige belastningen, med mindre ansvaret kan lempes, se lovutkastet § 37c.

Etter *annet punktum* gjelder heller ikke ansvarsgrensene ved feilbruk som følge av at kontohaveren eller noen som nødvendig brukerlegitimasjon er overlatt til, da betalingsordren ble gitt, bevisst har oversett en særskilt varslingsordning etablert for å hindre slik feilbruk. Det vises til avsnitt 6.3.3 foran.

Etter *tredje punktum* gjelder heller ikke ansvarsgrensene for tap som har oppstått som følge av at kontohaveren eller noen som nødvendig brukerlegitimasjon er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at det har skjedd feilbruk eller misbruk av den nettbaserte betalingstjenesten. I en slik situasjon fremstår det som urimelig at korthaveren skal være beskyttet av den aktuelle beløpsgrensen. I et system hvor banken er pliktig til å tilbakeføre overført beløp som kunden hevder er urettmessig eller utilsiktet, vil det være av viktighet at institusjonen så tidlig som mulig blir varslet

om forholdet og kan iverksette de tiltak som er nødvendig for å forsøke å rette opp situasjonen, slik at tapet om mulig kan begrenses.

I utkastets *femte ledd* er det slått fast at § 34 tredje og fjerde ledd gjelder tilsvarende. Det vises til avsnitt 6.3.3 og 6.3.4 foran.

Sjette ledd første punktum bestemmer at institusjonen kan kreve tilbakebetaling av tredjemann av betalingsmidler som denne urettmessig har mottatt som følge av feilbruk eller misbruk av nettbasert betalingstjeneste. Etter *annet punktum* skal tilbakebetalt beløp som overstiger institusjonens tap, benyttes til å dekke kontohaverens egenandel av tapet. Regelen skal forhindre at kunden – på uhensiktsmessig vis – blir straffet for sin skjødesløse handlingsmåte ved behandling av betalingsoppdraget når bankinstitusjonen har lykkes i å inndrive pengene. I forhold til tilfelle av urettmessig bruk antar *Banklovkommisjonen* at regelen ikke er like anvendelig som for de utilsiktede betalingstransaksjonene. Misbruk av nettbaserte betalingsoverføringer er ofte et utslag av et målrettet angrep hvor gjerningspersonen(e) har sørget for at kundens penger blir flyttet til konto i utlandet som de norske bankinstitusjoner nærmest har ingen mulighet til å spore opp og få tilbakeført. De utilsiktede transaksjonene vil på den annen side normalt manifestere seg i overføringer til en intetanende bankkunde uten i utgangspunktet kriminelle hensikter. Her vil antagelig bankinstitusjonen med enklere midler ha mulighet til å inndrive pengene.

Banklovkommisjonen har sett det som rimelig at bankinstitusjonen får dekket sitt økonomiske tap som følge av inndrivelsen, slik at det kun er tilbakebetalt beløp som overstiger institusjonens tap som skal benyttes til å dekke kontohaverens egenandel av tapet. Dette kan være arbeid for å få til et forlik med den uberettigede mottakeren og andre kostnader i tilknytning til tilbakeføring av pengene til kunden.

Til § 37c. Lemping av kontohaverens ansvar

Etter *første ledd første punktum* kan ansvaret etter § 37b lempes dersom ansvaret etter forholdene vil virke urimelig tyngende for kunden. Det skal her tas hensyn til om måten kontoen kan disponeres på ikke er betryggende, og om den nettbaserte betalingstjenesten er i samsvar med forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner, dersom den utilsiktede eller urettmessige betalingsoverføringen har sammenheng med slike forhold. Denne vurderingen vil kunne knyttes opp mot avgjørelsen av om kunden har opptrådt grovt uaktsomt. Dersom det har vært en viss usikkerhet med henhold til i hvilken utstrekning den nettbaserte betalingstjenesten gir slik sikkerhet mot feilbruk eller misbruk som en bruker eller allmennheten med rimelighet kan vente, antar *Banklovkommisjonen* at et ansvar på grunnlag av grov uaktsomhet, enten etter annet eller fjerde ledd, lettere vil kunne lempes.

Etter *annet punktum* kan det også tas hensyn til manglende aktsomhet eller andre forhold på institusjonens side som har medvirket til at den urettmessige eller utilsiktede betalingsoverføringen ble utført. Manglende eller utilstrekkelig veiledning fra institusjonens side vil her kunne være en relevant faktor. Igjen vil dette være et forhold som kan trekkes inn allerede i vurderingen av om kunden har opptrådt grovt uaktsomt og medføre lemping av kundens eventuelle forhøyede egenandel.

Banklovkommisjonen viser for øvrig til avsnitt 6.3.5 foran.

Til § 37d. Reklamasjon. Tilbakeføring

Bestemmelsen svarer hovedsakelig til finansavtaleloven § 37. Ettersom regelen om reklamasjon og tilbakeføring gjelder for både de utilsiktede og urettmessige transaksjonene, har *Banklovkommisjonen* imidlertid ansett det nødvendig å utdype kravet til dokumentasjon noe.

Etter *første ledd* er det bestemt at tilbakeføring av et beløp kunden bestrider å ha ansvar for forutsetter at kunden fremsetter et begrunnet krav om slik tilbakeføring. Kontohaveren plikter i tillegg å gi opplysninger til institusjonen om, og på hvilken måte, det er gjort forsøk på å få betalingsmottakeren til å tilbakeføre beløp som utilsiktet eller urettmessig er overført til mottakeren, jf. *annet ledd.* Det vises for øvrig til avsnitt 6.3.6 punkt 2) foran. Ut fra en slik reklamasjon vil institusjonen ha et bedre vurderingsgrunnlag i forhold til om kunden kan sies å ha gått frem på en måte som enten anses som unnskyldelig, grov uaktsom eller forsettlig, og vil dessuten avhjelpe institusjonens vurdering av om saken bør bringes inn for nemnd- eller domstolsbehandling.

Kapittel 9
Utkast til endring i finansavtaleloven av 25. juni 1999 nr. 46 kapittel 2

[Banklovkommisjonens utkast til endring er markert med kursiv.]

V. *Andres misbruk av konto mv.*

§ 34. *Misbruk av konto m.v.*

(1) Kontohaveren er ikke ansvarlig for andres urettmessige uttak eller annen belastning med mindre den som har foretatt disposisjonen, har legitimert seg i samsvar med reglene i kontoavtalen, og belastningen har vært mulig som følge av forsett eller grov uaktsomhet fra kontohaveren eller fra noen som etter kontoavtalen har rett til å belaste kontoen.

(2) Ansvaret etter første ledd er begrenset til disponibelt beløp på kontoen på belastningstidspunktet. Er misbruk skjedd ved bruk av elektroniske betalingsinstrumenter innenlands, kan ansvaret heller ikke overskride belastningsgrenser som gjelder for den eller de bruksmåter som er benyttet. Begrensningene i leddet her gjelder ikke dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har medvirket forsettlig til at vedkommende kunne legitimere seg.

(3) Kontohaveren svarer ikke for andres urettmessige bruk som finner sted etter at institusjonen har fått varsel om forhold som skaper særlig fare for misbruk, som f.eks. at et betalingsinstrument er kommet bort eller at kode eller annen sikkerhetsprosedyre kan ha blitt tilgjengelig for uvedkommende. Kontohaveren er likevel ansvarlig dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, forsettlig har muliggjort bruken.

(4) Uten hensyn til reglene i denne paragrafen er kontohaveren i alle tilfelle ansvarlig for tap som skyldes at kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har utvist eller medvirket til svik mot institusjonen.

(5) Ansvaret ved misbruk av betalingskort er regulert i § 35. *Ansvaret ved utilsiktet eller urettmessig betalingsoverføring ved bruk av annen nettbasert betalingstjeneste er regulert i § 37a til § 37d.*

Va. *Feilbruk og misbruk av ordninger for nettbasert betalingsoverføring*

§ 37a. *Virkeområde*

(1) Bestemmelsene i dette avsnitt gjelder betalingsoverføring ved bruk av nettbaserte betalingstjenester, unntatt betalingsoverføring ved bruk av betalingskort.

(2) Med nettbasert betalingsoverføring forstås her overføring av betalingsmidler fra innskuddskonto i henhold til betalingsoppdrag sendt til og mottatt av institusjonen gjennom Internett eller annet elektronisk nettverk.

(3) Med nettbasert betalingstjeneste forstås her ordning for nettbasert betalingsoverføring i henhold til avtale mellom kontohaveren og institusjonen, herunder nettbank- og telefonbanktjenester.

(4) Bestemmelsene i §§ 37b til 37d kan ikke fravikes ved avtale til skade for kontohaveren. Dersom en institusjon som tilbyr nettbasert betalingstjeneste, også har etablert en særskilt nettbasert betalingstjeneste bare for næringslivskunder, kan bestemmelsene i §§ 37b til 37d likevel fravikes i avtalen mellom institusjonen og kontohaveren om tilgang til slik særskilt betalingstjeneste. Kongen kan i forskrift fastsette nærmere regler om hvilke kontohavere som her skal regnes som næringslivskunder.

§ 37b. *Utilsiktet og urettmessig bruk av nettbasert betalingstjeneste*

(1) Kontohaveren svarer med en egenandel på inntil kr 1.200 for tap som følge av utilsiktet eller urettmessig betalingsoverføring ved feilbruk eller misbruk av nettbasert betalingstjeneste når personlig kode og annen lignende sikkerhetsprosedyre eller sikkerhetsverktøy (nødvendig brukerlegitimasjon) er brukt for å få utført et betalingsoppdrag. Dette gjelder likevel ikke dersom tapet skyldes at institusjonens nettbaserte betalingstjeneste ikke byr den sikkerhet mot feilbruk eller misbruk som en bruker eller allmennheten med rimelighet kunne vente, eller at en tredjemann ved inntrenging i elektronisk nettverk, grov tvang eller lignende handlemåte urettmessig har skaffet seg tilgang til nødvendig brukerlegitima-

sjon eller endret det betalingsoppdrag kontohaveren har gitt.

(2) Kontohaveren svarer med inntil kr 12.000 for tap som følge av utilsiktet eller urettmessig betalingsoverføring i tilfelle som nevnt i første ledd når betalingsoverføringen er gjort mulig ved grov uaktsomhet av kontohaveren, eller av noen som nødvendig brukerlegitimasjon er overlatt til. Det samme gjelder dersom misbruk er muliggjort fordi kontohaveren eller noen nødvendig brukerlegitimasjon er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at brukerlegitimasjonen er kommet bort eller må ha kommet på avveie, eller innen rimelig tid etter at dette burde være oppdaget

(3) Ved avgjørelsen av om betalingsoverføringen er gjort mulig ved grov uaktsomhet som nevnt i annet ledd, skal det blant annet legges vekt på om slike krav til forsiktighet og egenkontroll som med rimelighet kan stilles til brukere av nettbaserte betalingstjenester, er blitt klart tilsidesatt, og i hvilken utstrekning den nettbaserte betalingstjenesten gir slik sikkerhet mot feilbruk eller misbruk som en bruker eller allmennheten med rimelighet kunne vente.

(4) Ansvarsgrensene etter første og annet ledd gjelder ikke tap som er oppstått ved feilbruk eller misbruk av den nettbaserte betalingstjenesten, og som er forsettlig voldt av kontohaveren eller noen som nødvendig brukerlegitimasjon er overlatt til. Ansvarsgrensen gjelder heller ikke ved feilbruk som følge av at kontohaveren eller noen som nødvendig brukerlegitimasjon er overlatt til, da betalingsordren ble gitt, bevisst har oversett en særskilt varslingsordning etablert for å hindre slik feilbruk. Det samme gjelder for tap som har oppstått som følge av at kontohaveren eller noen som nødvendig brukerlegitimasjon er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at det har skjedd feilbruk eller misbruk av den nettbaserte betalingstjenesten.

(5) § 34 tredje og fjerde ledd gjelder tilsvarende for kontohaverens ansvar etter paragrafen her.

(6) Institusjonen kan kreve tilbakebetaling av tredjemann av betalingsmidler som denne urettmessig har mottatt som følge av feilbruk eller misbruk av nettbasert betalingstjeneste som omfattes av paragrafen her. Tilbakebetalt beløp som overstiger institusjonens tap, skal benyttes til å dekke kontohaverens egenandel av tapet.

§ 37c. Lemping av kontohaverens ansvar

(1) Ansvaret etter § 37b kan lempes dersom ansvaret etter forholdene vil virke urimelig tyngende for kontohaveren. Det skal tas hensyn til om måten kontoen kan disponeres på ikke er betryggende, og om den nettbaserte betalingstjenesten er i samsvar med forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner, dersom den utilsiktede eller urettmessige betalingsoverføringen har sammenheng med slike forhold. Det kan også tas hensyn til manglende aktsomhet eller andre forhold på institusjonens side som har medvirket til at den urettmessige eller utilsiktede betalingsoverføringen ble utført.

§ 37d. Reklamasjon. Tilbakeføring

(1) I den utstrekning kontohaveren bestrider å ha ansvar for en betalingsoverføring, skal institusjonen tilbakeføre beløpet etter fradrag av egenandelen etter § 37b første ledd, samt erstatte rentetap fra belastningstidspunktet, forutsatt at kontohaveren setter frem begrunnet krav om tilbakeføring uten ugrunnet opphold etter at denne ble eller burde ha blitt kjent med forholdet.

(2) Kontohaveren plikter å gi opplysninger til institusjonen om, og på hvilken måte, det er gjort forsøk på å få betalingsmottakeren til å tilbakeføre beløp som utilsiktet eller urettmessig er overført til mottakeren.

(3) Første ledd gjelder ikke dersom

a) kontohaveren skriftlig har erkjent ansvar for betalingsoverføringen, eller

b) institusjonen innen fire uker fra mottakelse av skriftlig innsigelse fra kontohaveren har anlagt søksmål eller brakt saken inn for en nemnd som nevnt i § 4 første ledd.

(4) Blir saken avvist av en nemnd eller en domstol, løper en ny frist på fire uker, fra den dagen institusjonen ble kjent med avvisningen.

Vedlegg 1

Oversikt over direktiv 2007/64/EF om betalingstjenester

1 Generelt om direktivet

Europaparlamentets og Rådets direktiv 2007/64/EF om betalingstjenester i EU ble vedtatt 13. november 2007. Direktivet endrer og opphever tidligere direktiv som vedrører betalingstjenester. Et utdrag av betalingstjenestedirektivet er inntatt i Vedlegg II. I fortalen til direktivet er det uttalt at det på nåværende tidspunkt er mangel på harmoniserende regler for betalingstjenester i den forstand at rammeverket for slike tjenester er oppdelt i 27 forskjellige nasjonale lovordninger. Det er i følge Europaparlamentet og Rådet helt nødvendig at det etableres moderne og samordnede regler for betalingstjenester innenfor Det europeiske fellesskap.

Hvilke betalingstjenester som er omfattet av direktivet, er regulert i et vedlegg til direktivet.[1] Her er det opplistet en rekke betalingstjenester, herunder innskudd, uttak, overføring via giro og kredittkort, pengeoverførselsvirksomhet (bankremisse) og betalingstransaksjoner utført gjennom blant annet Internett (nettbanktjenesten). Direktivet er avgrenset mot sjekk, «cash to cash»-overføringer og lignende, se artikkel 3.[2] Det er særlig betalingsoverføring ved hjelp av giro, kredittkort og nettbank som utpeker seg.

Direktivet angir hvilke foretak som kan utføre betalingsoverføring. I artikkel 1 bokstav a) til f), er det oppregnet seks typer av *betalingsoverføringsforetak*. Dette er blant annet kredittinstitusjoner som er omfattet av direktiv 2006/48/EF (det konsoliderte bankdirektiv), e-pengeforetak omfattet av direktiv 2000/46/EF,[3] postgirokontorer, den europeiske sentralbanken og nasjonale sentralbanker, samt medlemsstater eller deres regionale og lokale myndigheter. De to sistnevnte typene (sentralbank og myndigheter) kan bare regnes som betalingsoverføringsovertak så framt de ikke handler i sin egenskap som offentlig myndighet. I tillegg til de ovennevnte institusjoner er også *betalingsforetak* omfattet av direktivet. Disse foretakene trenger særskilt konsesjon som er nærmere regulert i direktivet. Her er det blant annet gitt regler om vilkår for tillatelse og virksomhetsbegrensninger, se avsnitt 2 nedenfor.

I det følgende benyttes *betalingsoverføringsforetak* som fellesbetegnelse for samtlige typer av foretak som tilbyr betalingstjenester (sml. direktivets definisjon av «payment service provider» i artikkel 4 nr. 9). *Betalingsforetak* er slikt sett forbeholdt de foretak som må søke om konsesjon etter direktivet (sml. direktivets definisjon av «payment institution» i artikkel 4 nr. 4).

Direktivet gir alle de seks typene av betalingsoverføringsforetak tilgang til betalingsoverføringssystemer, se artikkel 28. Denne tilgangen skal skje på basis av objektive, ikke-diskriminerende og proporsjonale nasjonale regler.

Av artikkel 29 følger at andre foretak enn de seks nevnte institusjonene i artikkel 1, ikke skal kunne utføre betalingstjenester. Direktivets rekkevidde i forhold til slike tjenester er som nevnt definert i vedlegg til direktivet.

I artikkel 4 er det gitt viktige definisjoner av begreper knyttet til betalingsoverføring og betalingstjenester. *Banklovkommisjonen* har ikke funnet grunn til å gå nærmere inn på de enkelte definisjoner. Noen definisjoner og henvisninger er likevel inntatt på ulike steder i denne oversikten.

Når det gjelder anvendelsesområdet for direktivet, er det i artikkel 2 fastsatt at det gjelder for betalingsoverføringer innenfor Det europeiske fellesskap. Virksomhetsregler og nærmere bestemmelser om rammeavtaler for bruk av betalingstjeneste gjelder bare når både betalerens og mottakerens tjenesteyter (det vil si betalingsoverføringsforetaket) er etablert innenfor fellesskapet.[4] De nevnte reglene gjelder alle overføringer i euro eller i medlemsstats valuta, men ikke overføringer i annen valuta, se artikkel 2 nr. 3.

De alminnelige virksomhetsreglene for foretak som utfører betalingsoverføringer er inntatt i artik-

[1] Jf. også definisjonen av «payment service» i artikkel 4 nr. 3.
[2] Se også fortalen punkt 6.
[3] Disse er for øvrig omfattet av definisjonen «credit institution» i det konsolidierte bankdirektiv, se artikkel 4 nr. 1 bokstav b).
[4] Avsnitt III («Transparency of conditions and information requirements for payment services») og IV («Rights and obligations in relation to the provision and use of payment services») i direktivet.

kel 30 til 50, se avsnitt 3, og regler for utføring av de enkelte betalingsoverføringer er inntatt i artikkel 51 til 83, se avsnitt 4 nedenfor.

Direktivet er i utgangspunktet et fullharmoniseringsdirektiv. Det er likevel inntatt flere minimumsbestemmelser som gjør det mulig for de enkelte lands myndigheter å fastsette strengere regler. Det handlingsrom som disse minimumsbestemmelsene legger opp til, skal blant annet utredes av arbeidsgruppen nedsatt av Finansdepartementet, jf. avsnitt 1.2.2 foran i utredningen om nettbankbasert betalingsoverføring. Visse regler i direktivet gjelder i utgangspunktet bare for forbrukere, slik at det er mulig for medlemsstatene å unnta visse av direktivets regler i forholdet mellom betalingsformidler og mer profesjonelle parter, se eksempelvis artikkel 30 og 51. Unntak kan også gjøres for betalinger av mindre størrelser. De regler som gjelder for dette er heller ikke drøftet nærmere, se for øvrig artikkel 53 flg.

I det følgende gis det en oversikt over hovedelementene som er regulert i direktivet. Det er forsøkt å identifisere temaene på et overordnet nivå uten å gå for mye inn i detaljene i de enkelte bestemmelsene. Det redegjøres først for konsesjonssystemet for betalingsforetak, se avsnitt 2. De overordnede virksomhetsreglene som gjelder for betalingsoverføringsforetak er gjennomgått i avsnitt 3. I avsnitt 4 nedenfor sees det nærmere på reglene for gjennomføring av betalingsoverføringer. En nærmere regulering av de mer materielle sidene ved, og tjenestene til, virksomheten er noe uvanlig. Dette viser at forbrukervernet er tillagt vesentlig vekt i forhold til visse betalingstjenester.

2 Konsesjonssystem for betalingsforetak

Konsesjonsregler for betalingsforetak er gitt i direktivets artikkel 5 til 27. I direktivets artikkel 5 er det angitt flere vilkår som må være oppfylt for at de kompetente myndigheter i medlemsstaten skal kunne godkjenne foretaket som et betalingsforetak. Disse avviker ikke i stor grad fra vilkår som stilles til finansforetak etter andre finansielle EU-direktiv, se også finansieringsvirksomhetsloven § 3-3. Det er blant annet inntatt vilkår om at søknaden skal inneholde forretningsplan, en beskrivelse av interne kontrollmekanismer og organisasjonsstruktur, en liste over personer i ledelsen mv.

Artikkel 6 vedrører kravene til startkapital. At disse kravene er oppfylt er et vilkår for å kunne få tillatelse, se artikkel 5 første ledd bokstav c). Kravene til startkapital varierer alt etter hva slags betalingstjenester foretaket vil tilby, se vedlegget til direktivet. Når det gjelder de komponenter som skal inngå i beregningen av startkapital, er det vist til direktiv 2006/48/EF (det konsoliderte bankdirektiv) artikkel 57 bokstav a) og b). *Banklovkommisjonen* går ikke nærmere inn på dette. Foretak som kun skal drive virksomhet med pengeoverføring, skal ha en startkapital på minimum 20 000 euro, jf. artikkel 6 bokstav a). For foretak som kun tilbyr betalingsoverføringer ved hjelp av telekommunikasjon, digitalt medium eller datasystem, skal ha en startkapital på minimum 50 000 euro, jf. bokstav b). Når det gjelder foretak som skal tilby et større spekter av betalingstjenester (angitt i vedlegget nr. 1-5), herunder de mer tradisjonelle betalingstjenester som innskudd og uttak, er det stilt som vilkår at foretaket har en startkapital på minimum 125 000 euro, jf. bokstav c).

I artikkel 9 er det bestemt at betalingsforetak som mottar midler fra bruker av betalingstjenesten («payment service user», se artikkel 4 nr. 10) skal ha betryggende rutiner og kontrollordninger for å beskytte midlene. At kravene i denne bestemmelsen er oppfylt, er også et vilkår for tillatelse, se artikkel 5 første ledd bokstav d). Det er lagt opp til at foretakene kan velge mellom ordninger med atskillelse av midlene mot for eksempel foretakets kreditorer eller at midlene dekkes av en betryggende forsikringsordning, se artikkel 9 nr. 1.

Dersom vilkårene etter artikkel 5, jf. artikkel 6 og 9 er oppfylt, kan det gis tillatelse til å drive virksomhet som betalingsforetak, jf. artikkel 10. Tillatelsen skal meddeles senest 3 måneder etter at søknad fra foretaket er mottatt, jf. artikkel 11. Det er imidlertid inntatt flere vilkår i selve meddelelsen av tillatelsen. Det er bestemt at tillatelse bare kan meddeles dersom det finnes effektive former for virksomhetsstyring av betalingstjenestevirksomheten. Dette innebærer blant annet at det foreligger en klar organisatorisk struktur med en veldefinert, gjennomskuelig og konsekvent ansvarsfordeling, jf. artikkel 10 nr. 4. Det kan stilles øvrige vilkår for utstedelse av tillatelse, blant annet om at foretaket oppretter en særskilt enhet for betalingsvirksomheten dersom foretakets andre aktiviteter enn betalingstjenester svekker eller kan svekke foretakets soliditet eller de kompetente myndigheters mulighet for å føre tilsyn med foretaket, jf. artikkel 10 nr. 5. Tillatelsen er også betinget av at foretaket ikke har «snevre forbindelser» med fremmed stat som kan svekke ivaretakelsen av tilsynsoppgavene, jf. artikkel 10 nr. 8.

3 Virksomhetsregler for betalingsoverføringsforetak

Direktivet inneholder en rekke virksomhetsregler. Disse gjelder for samtlige typer av institusjoner som er oppregnet i artikkel 1 nr. 1. De fleste avvikker ikke i stor grad fra virksomhetsbestemmelser for andre finansielle foretak som opererer innenfor Det europeiske fellesskap. Det er imidlertid inntatt en del spesifikke bestemmelser vedrørende de enkelte betalingsoverførignene. Selv om disse er å anse som virksomhetsregler, er de utelatt i denne sammenheng og behandlet nærmere i avsnitt 4 nedenfor.

Direktivet har for det første regler om at virksomheten drives i henhold til de angitte vilkårene for å kunne drive betalingstjenestevirksomhet, jf. artikkel 14. Dersom det skjer en endring i foretaket som vil påvirke den informasjonen som foretaket har avgitt i henhold til artikkel 5, skal de kompetente myndigheter i medlemsstaten varsles.

Det er videre gitt regler om tillatelse til å drive annen eller tilknyttet virksomhet. Utgangspunktet er at det gis tillatelse til å drive virksomhet som faller inn under definisjonen av betalingstjeneste i vedlegget til direktivet. Etter artikkel 16 er det for øvrig angitt andre typer virksomhet som likevel er tillatt. Dette vedrører blant annet muligheten til å drive tilknyttet virksomhet slik som valutaveksling, depottjenester, samt lagring og behandling av data, jf. artikkel 16 nr. 1 bokstav a).

Det er også gitt regler om bruk av agenter, filialer eller enheter hvor virksomhetens betalingstjenester er «outsourced», jf. artikkel 17 flg.

Krav til foretakets kapitaldekning må for det første sees i sammenheng med kravene til startkapital, jf. artikkel 6. I artikkel 7 er det bestemt at den ikke skal falle under startkapitalen som angitt i artikkel 6, se også avsnitt 2 foran. Videre er det stilt krav om at egenkapitalen ikke skal falle under et beløp etter nærmere angitte beregningsmetoder av egenkapital, se artikkel 7 nr. 1, jf. artikkel 8. Det er de nasjonale myndigheter som bestemmer hvilken beregningsmetode som skal tas i bruk, jf. artikkel 8 nr. 1.

Det er videre gitt regler for informasjon som skal gis til bruker av betalingstjenesten. Det er her skilt mellom kontrakter som bruker inngår for engangsoverføringer («single payment contract») og rammekontrakter (eksempelvis nettbankavtale). I det følgende er det tatt utgangspunkt i informasjonskrav i forhold til rammekontrakter. Når det gjelder informasjon som skal gis til bruker, dreier det seg først og fremst om navn på tilbyder av tjenesten, dennes adresse og øvrig kontaktinformasjon, jf. artikkel 42 nr. 1 bokstav a).

I tilknytning til bruk av betalingstjenesten skal foretaket i nærmere detalj beskrive hva slags tjeneste som tilbys, se artikkel 42 nr. 2 bokstav a). Foretaket skal videre utgi en «unique indentifier» som er nødvendig for at betalingsoverføring kan utføres, jf. bokstav b). «Unique identifier» er definert som «a combination of letters, numbers or symbols specified to the payment sevice user by the payment service provider and to be provided by the payment service user to identify unambiguously to the other payment service user and/or his payment account for a payment transaction», jf. Artikkel 4 nr. 21. I dette ligger et krav om at foretaket skal gi brukeren en kode som utvetydig skal kunne identifisere betalingsmottageren eller dennes konto. Dette vil typisk være oppfylt ved at betalingsoverføringsforetaket utgir kontonummer eller IBAN-nummer til brukeren. Videre skal det informeres om maksimum behandlingstid for betalingsordre, se artikkel 42 nr. 2 bokstav e).

Eventuelle gebyrer for bruk av tjenesten skal formidles til brukeren, jf. artikkel 42 nr. 3 bokstav a). Foretaket skal også informere om frister for melding av uautoriserte betalingsordre som brukeren blir oppmerksom på, jf. nr. 5 bokstav d). Dette er regulert nærmere i artikkel 58. De nærmere informasjonspliktene relatert til betalingsoverføringer er redegjort for i avsnitt 4 nedenfor.

4 Utførelse av betalingsoverføringer

Det er inntatt en rekke bestemmelser som gjelder den spesifikke gjennomføringen av en betalingsoverføring. Det dreier seg om regler før, under og etter at en betalingstransaksjon er utført. Reglene som knytter seg til før en betalingsoverføring er utført, omhandler i første rekke informasjon fra foretak til kunde og er gjennomgått i avsnittet foran.

Foretaket skal gi informasjon til brukeren etter at beløpet er trukket fra kontoen. Det dreier seg om informasjon om hvem pengene er overført til, det eksakte beløpet som er overført, eventuelle gebyrer, eventuell valutarate og dato for når betalingsordren ble bestilt, jf. artikkel 47 nr. 1. Informasjonen skal formidles slik at brukeren har mulighet til å lagre den, jf. artikkel 47 nr. 2. Medlemsstatene kan likevel kreve at slik informasjon skal formidles per post og ikke elektronisk, jf. artikkel 47 nr. 3. Mer eller mindre tilsvarende bestemmelser skal gjelde for betalingsmottaker, jf. artikkel 48.

Et viktig tema er samtykke til gjennomføring av en betaling. Medlemsstatene er pålagt å utforme

regler som innebærer at det må gis samtykke før betaling kan gjennomføres, se artikkel 54 nr. 1. Slikt samtykke skal gjøres på en måte som er avtalt mellom betalingsformidleren og betaleren.

Når betalingen er gjennomført, skal betaleren motta kvittering på betalingsoverføringen. Det er gitt regler om frister for dette og når betaling skal anses å ha funnet sted, se artikkel 64. Når slik informasjon er utsendt til betaleren, er det videre oppstilt krav til når pengene skal krediteres betalingsmottagerens konto, se artikkel 69. For nasjonale betalingsoverføringer er det lagt opp til at nasjonale myndigheter kan innføre kortere frister enn det som er angitt i direktivet, se artikkel 72.

Direktivet inneholder også regler om tilbakekalling av betalingsordre. Utgangspunktet er at det ikke er mulig å tilbakekalle en betalingsordre når denne er mottatt av «payment service provider», jf. artikkel 66 nr. 1. Det er imidlertid oppført noen unntak fra dette. Betaleren kan forhindre at betalingen utføres dersom det er betalingsmottageren som har initiert betalingsordren. Dette gjelder frem til betaleren gir sitt samtykke til betalingsmottagers forespørsel om overføring, jf. artikkel 66 nr. 2. For avtaler om direkte debitering, kan betalingen likevel tilbakekalles så lenge dette gjøres dagen før tidspunktet som er avtalt for debitering av betalerens konto, jf. artikkel 66 nr. 3. De sistnevnte tilfellene krever for øvrig at betalingsmottageren samtykker i tilbakekallingen, jf. artikkel 66 nr. 5.

Beløpet som skal gjennomføres, skal som utgangspunkt ikke være belagt med gebyrer, med mindre dette er avtalt mellom partene, se artikkel 67.

Det er særlig ansvarsreguleringen rundt såkalte uautoriserte betalingstransaksjoner som er fremhevet i direktivet. Så lenge brukeren gir melding om slike uautoriserte transaksjoner innen visse tidsfrister, holdes betalingsformidlingsforetaket som utgangspunkt ansvarlig for det beløp som er debitert kontoen til brukeren, jf. artikkel 60, se artikkel 58 og 59. Etter artikkel 61 holdes imidlertid brukeren ansvarlig for uautoriserte betalingstransaksjoner opp til et maksimumsbeløp på 150 euro. Det er videre bestemt at brukeren skal dekke alle tap dersom den uautoriserte overføringen skyldes svikaktig handling eller med forsett eller grov uaktsomhet har handlet i strid med reglene om bruk av betalingstjenesten eller meldingsplikten, se artikkel 61 nr. 2, jf. artikkel 56.

Selv om brukeren har handlet grovt uaktsomt i forhold til sine plikter til foreskrevet bruk av betalingstjenesten og melding om tap, tyveri eller uberettiget tilegnelse av betalingsinstrumentet, kan ansvaret reduseres med hensyntagen til betalingsoverføringsforetakets sikkerhetsordninger og de omstendigheter som førte til tap, tyveri eller uberettiget tilegnelse, jf. artikkel 61 nr 3.

Det stilles i denne sammenheng krav til at betalingsformidleren har tilfredsstillende forordninger for mottagelse av meldinger fra bruker som nevnt foran, jf. artikkel 61 nr 5. Dersom dette ikke er tilfelle, kan ikke bruker holdes ansvarlig med mindre han har opptrådt svikaktig.

Det er også gitt regler om tilbakeføring av beløp som er overført ved betalingsordre initiert av betalingsmottager, se artikkel 62 flg. Dette gjelder for det første der betalingsordren fra betalingsmottageren ikke spesifiserte beløpet eller beløpet overskred det som betaleren med rimelighet kunne vente ut fra tidligere utgiftsmønstre. Betaleren er imidlertid pålagt å frembringe opplysninger om disse forholdene dersom betalingsformidleren krever det. Det er også gitt regler om anmodning om tilbakeføring av betalingstransaksjoner som er initiert av en betalingsmottager, se artikkel 63.

Det er videre fastslått visse regler knyttet til «unique indentifier» som er nødvendig for at betalingsoverføring kan utføres. I dette ligger som nevnt i avsnitt 3 foran, et krav om at foretaket skal gi brukeren en kode som utvetydig skal kunne identifisere betalingsmottageren eller dennes konto. Dette vil typisk være betalingsmottagerens kontonummer. I artikkel 74 nr. 1 er det bestemt at et betalingsoppdrag som er utført i samsvar med de instruksjoner som institusjonen har mottatt, «shall be deemed to have been executed correctly», det vil si skal anses som korrekt utført av institusjonen. Bestemmelsen kan i og for seg tyde på at kontohaveren skal bære det fulle ansvar for tap som måtte oppstå i tilfelle hvor det har skjedd en utilsiktet betalingsoverføring som følge av brukerfeil fra kontohavens side. På bakgrunn av fortalens paragrafer 32 og 34 forstår *Banklovkommisjonen* denne bestemmelsen slik at den ikke utgjør en uavbeviselig lovpresumpsjon, og at bestemmelsen derfor ikke er til hinder for ansvar for institusjonen i tilfelle hvor brukerfeilen eller den utilsiktede betalingsoverføringen har sin bakgrunn i at sikkerhets- og veiledningsnivået i den nettbaserte betalingstjenesten ikke kan anses tilstrekkelig til å forebygge slike forhold. Det vises for så vidt til bemerkningene i avsnitt 6.2.3 punkt 3) foran vedrørende forståelsen av direktivets formålsparagrafer 32 og 34.

Vedlegg 2

Utdrag av betalingstjenestedirektivet, Rdir. 2007/64/EF

DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 November 2007

on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular the first and third sentences of Article 47(2) and Article 95 thereof,

Having regard to the proposal from the Commission,

Having consulted the European Economic and Social Committee,

Having regard to the opinion of the European Central Bank,

Acting in accordance with the procedure laid down in Article 251 of the Treaty,

Whereas:

(1) It is essential for the establishment of the internal market that all internal frontiers in the Community be dismantled so as to enable the free movement of goods, persons, services and capital. The proper operation of the single market in payment services is therefore vital. At present, however, the lack of harmonisation in this area hinders the operation of that market.

(2) Currently, the payment services markets of the Member States are organised separately, along national lines and the legal framework for payment services is fragmented into 27 national legal systems.

(3) Several Community acts have already been adopted in this area, namely Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers and Regulation (EC) No 2560/2001 of the European Parliament and of the Council of 19 December 2001 on cross-border payments in euro, but these have not sufficiently remedied this situation any more than have Commission Recommendation 87/598/EEC of 8 December 1987 on a European Code of Conduct relating to electronic payment (relations between financial institutions, traders and service establishments, and consumers), Commission Recommendation 88/590/EEC of 17 November 1988 concerning payment systems, and in particular the relationship between cardholder and card issuer, or Commission

Figur 2.1

Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder. These measures continue to be insufficient. The co-existence of national provisions and an incomplete Community framework gives rise to confusion and a lack of legal certainty.

(4) It is vital, therefore, to establish at Community level a modern and coherent legal framework for payment services, whether or not the services are compatible with the system resulting from the financial sector initiative for a single euro payments area, which is neutral so as to ensure a level playing field for all payment systems, in order to maintain consumer choice, which should mean a considerable step forward in terms of consumer cost, safety and efficiency, as compared with the present national systems.

(5) That legal framework should ensure the coordination of national provisions on prudential requirements, the access of new payment service providers to the market, information requirements, and the respective rights and obligations of payment services users and providers. Within that framework, the provisions of Regulation (EC) No 2560/2001, which created a single market for euro payments as far as prices are concerned, should be maintained. The provisions of Directive 97/5/EC and the recommendations made in Recommendations 87/598/EEC, 88/590/EEC and 97/489/EC should be integrated in a single act with binding force.

(6) However, it is not appropriate for that legal framework to be fully comprehensive. Its application should be confined to payment service providers whose main activity consists in the provision of payment services to payment service users. Nor is it appropriate for it to apply to services where the transfer of funds from the payer to the payee or their transport is executed solely in bank notes and coins or where the transfer is based on a paper cheque, paper-based bill of exchange, promissory note or other instrument, paper-based vouchers or cards drawn upon a payment service provider or other party with a view to placing funds at the disposal of the payee. Furthermore, a differentiation should be made in the case of means offered by telecommunication, information technology or network operators to facilitate purchasing of digital goods or services, such as ring tones, music or digital newspapers, besides traditional voice services and their distribution to digital devices. The content of these goods or services may be produced either by a third party or by the operator, who may add intrinsic value to them in the form of access, distribution or search facilities. In the latter case, where the goods or services are distributed by one of those operators, or, for technical reasons, by a third party, and where they can be used only through digital devices, such as mobile phones or computers, that legal framework should not apply as the activity of the operator goes beyond a mere payment transaction. However, it is appropriate for that legal framework to apply to cases where the operator acts only as an intermediary who simply arranges for payment to be made to a third-party supplier.

(7) Money remittance is a simple payment service that is usually based on cash provided by a payer to a payment service provider, which remits the

Figur 2.2

corresponding amount, for example via communication network, to a payee or to another payment service provider acting on behalf of the payee. In some Member States supermarkets, merchants and other retailers provide to the public a corresponding service enabling the payment of utility and other regular household bills. Those bill-paying services should be treated as money remittance as defined in this Directive, unless the competent authorities consider the activity to fall under another payment service listed in the Annex.

(8) It is necessary to specify the categories of payment service providers which may legitimately provide payment services throughout the Community, namely, credit institutions which take deposits from users that can be used to fund payment transactions and which should continue to be subject to the prudential requirements under Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, electronic money institutions which issue electronic money that can be used to fund payment transactions and which should continue to be subject to the prudential requirements under Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking-up, pursuit and prudential supervision of the business of electronic money institutions, and post office giro institutions which are so entitled under national law.

(9) This Directive should lay down rules on the execution of payment transactions where the funds are electronic money, as defined in Article 1(3)(b) of Directive 2000/46/EC. This Directive should, however, neither regulate issuance of electronic money nor amend the prudential regulation of electronic money institutions as provided for in Directive 2000/46/EC. Therefore, payment institutions should not be allowed to issue electronic money.

(10) However, in order to remove legal barriers to market entry, it is necessary to establish a single licence for all providers of payment services which are not connected to taking deposits or issuing electronic money. It is appropriate, therefore, to introduce a new category of payment service providers, "payment institutions", by providing for the authorisation, subject to a set of strict and comprehensive conditions, of legal persons outside the existing categories to provide payment services throughout the Community. Thus, the same conditions would apply Community-wide to such services.

(11) The conditions for granting and maintaining authorisation as payment institutions should include prudential requirements proportionate to the operational and financial risks faced by such bodies in the course of their business. In this connection, there is a need for a sound regime of initial capital combined with ongoing capital which could be elaborated in a more sophisticated way in due course depending on the needs of the market. Due to the range of variety in the payments services area, this Directive should allow various methods combined with a certain range of supervisory discretion to ensure that the same risks are treated the same way for all payment service providers. The requirements for the payment institutions should reflect the fact that payment institutions engage in more specialised and limited activities, thus generating risks that are narrower and easier to monitor and control than

Figur 2.3

those that arise across the broader spectrum of activities of credit institutions. In particular, payment institutions should be prohibited from accepting deposits from users and permitted to use funds received from users only for rendering payment services. Provision should be made for client funds to be kept separate from the payment institution's funds for other business activities. Payment institutions should also be made subject to effective anti-money laundering and anti-terrorist financing requirements.

(12) Payment institutions should draw up their annual and consolidated accounts in accordance with Council Directive 78/660/EEC of 25 July 1978 on the annual accounts of certain types of companies and, where applicable, Council Directive 83/349/EEC of 13 June 1983 on consolidated accounts and Council Directive 86/635/EEC of 8 December 1986 on the annual accounts and consolidated accounts of banks and other financial institutions. The annual accounts and consolidated accounts should be audited, unless the payment institution is exempted from this obligation under Directive 78/660/EEC and, where applicable, Directives 83/349/EEC and 86/635/EEC.

(13) This Directive should regulate the granting of credit by payment institutions, i.e. the granting of credit lines and the issuance of credit cards, only where it is closely linked to payment services. Only if credit is granted in order to facilitate payment services and such credit is of a short-term nature and is granted for a period not exceeding twelve months, including on a revolving basis, is it appropriate to allow payment institutions to grant such credit with regard to their cross-border activities, on condition that it is refinanced using mainly the payment institution's own funds, as well as other funds from the capital markets, but not the funds held on behalf of clients for payment services. The above should be without prejudice to Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit or other relevant Community or national legislation regarding conditions for granting credit to consumers not harmonised by this Directive.

(14) It is necessary for the Member States to designate the authorities responsible for granting authorisations to payment institutions, carrying out controls and deciding on the withdrawal of those authorisations. In order to ensure equality of treatment, Member States should apply to payment institutions no requirements other than those provided for in this Directive. However, all decisions made by the competent authorities should be contestable before the courts. In addition, the tasks of the competent authorities should be without prejudice to the oversight of payment systems, which, in line with the fourth indent of Article 105(2) of the Treaty, is a task to be carried out by the European System of Central Banks.

(15) Given the desirability of registering the identity and whereabouts of all persons providing remittance services and of according them all a measure of acceptance, irrespective of whether they are able to meet the full range of conditions for authorisation as payment institutions, so that none are forced into the black economy and bring all persons providing remittance service within the ambit of certain minimum legal and regulatory requirements, it is

Figur 2.4

appropriate and in line with the rationale of Special Recommendation VI of the Financial Action Task Force on Money Laundering to provide a mechanism whereby payment service providers unable to meet all those conditions may nevertheless be treated as payment institutions. For those purposes, Member States should enter such persons in the register of payment institutions while not applying all or part of the conditions for authorisation. However, it is essential to make the possibility of waiver subject to strict requirements relating to the volume of payment transactions. Payment institutions benefiting from a waiver should have neither the right of establishment nor the freedom to provide services, nor should they indirectly exercise those rights when being a member of a payment system.

(16) It is essential for any payment service provider to be able to access the services of technical infrastructures of payment systems. Such access should, however, be subject to appropriate requirements in order to ensure integrity and stability of those systems. Each payment service provider applying for a participation in a payment system should furnish proof to the participants of the payment system that its internal arrangements are sufficiently robust against all kinds of risk. These payment systems typically include e.g. the four-party card schemes as well as major systems processing credit transfers and direct debits. In order to ensure equality of treatment throughout the Community as between the different categories of authorised payment service providers, according to the terms of their licence, it is necessary to clarify the rules concerning access to the provision of payment services and access to payment systems. Provision should be made for the non-discriminatory treatment of authorised payment institutions and credit institutions so that any payment service provider competing in the internal market is able to use the services of the technical infrastructures of these payment systems under the same conditions. It is appropriate to provide for different treatment for authorised payment service providers and for those benefiting from a waiver under this Directive as well as from the waiver under the Article 8 of the Directive 2000/46/EC, due to the differences in their prudential framework. In any case differences in price conditions should be allowed only when this is motivated by differences in costs induced by the payment service providers. This should be without prejudice to Member States' right to limit access to systemically important systems in accordance with Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems and without prejudice to the competence of the European Central Bank and the European System of Central Banks (ESCB), as laid down in Article 105(2) of the Treaty and Article 3(1) and Article 22 of the Statute of the ESCB, concerning access to payment systems.

(17) The provisions of the access to payment systems should not apply to systems set up and operated by a single payment service provider. Those payment systems can operate either in direct competition to payment systems, or, more typically, in a market niche not adequately covered by payment systems. They typically cover three-party schemes, such as three party card schemes, payment services offered by telecommunication providers or money remittance services where the scheme operator is the payment service provider

Figur 2.5

to both the payer and payee as well as internal systems of banking groups. In order to stimulate the competition that can be provided by such payment systems to established mainstream payment systems, it should in principle not be appropriate to grant third parties access to these payment systems. Nevertheless, such systems should always be subject to Community and national competition rules which may require that access be granted to the schemes in order to maintain effective competition in payments markets.

(18) A set of rules should be established in order to ensure transparency of conditions and information requirements for payment services.

(19) This Directive should apply neither to payment transactions made in cash since a single payments market for cash already exists nor to payment transactions based on paper cheques since, by their nature, they cannot be processed as efficiently as other means of payment. Good practice in this area should, however, be based on the principles set out in this Directive.

(20) As consumers and enterprises are not in the same position, they do not need the same level of protection. While it is important to guarantee consumers' rights by provisions which cannot be derogated from by contract, it is reasonable to let enterprises and organisations agree otherwise. However, Member States should have the possibility to provide that micro-enterprises, as defined by Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, should be treated in the same way as consumers. In any case, certain core provisions of this Directive should always be applicable irrespective of the status of the user.

(21) This Directive should specify the obligations on payment service providers as regards the provision of information to the payment service users who should receive the same high level of clear information about payment services in order to make well-informed choices and be able to shop around within the EU. In the interest of transparency this Directive should lay down the harmonised requirements needed to ensure that necessary and sufficient information is given to the payment service users with regard to the payment service contract and the payment transactions. In order to promote smooth functioning of the single market in payment services, Member States should be able to adopt only those information provisions laid down in this Directive.

(22) Consumers should be protected against unfair and misleading practices in line with Directive 2005/29/EC of the European Parliament and the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the Internal Market as well as Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) and Directive 2002/65/EC of the European Parliament and the Council of 23 September 2002 concerning the distance marketing of consumer financial services. The additional provisions in those Directives continue to be applicable. However, the relationship of the pre-contractual information requirements between this Directive and Directive 2002/65/EC should, in particular, be clarified.

Figur 2.6

(23) The information required should be proportionate to the needs of users and communicated in a standard manner. However, the information requirements for a single payment transaction should be different from those of a framework contract which provides for the series of payment transactions.

(24) In practice, framework contracts and the payment transactions covered by them are far more common and economically important than single payment transactions. If there is a payment account or a specific payment instrument, a framework contract is required. Therefore, the requirements for prior information on framework contracts should be quite comprehensive and information should always be provided on paper or on another durable medium, such as printouts by account printers, floppy disks, CD-ROMs, DVDs and hard drives of personal computers on which electronic mail can be stored, and Internet sites, as long as such sites are accessible for future reference for a period of time adequate for the purposes of information and allow the unchanged reproduction of the information stored. However, it should be possible for the payment service provider and the payment service user to agree in the framework contract on the manner in which subsequent information on executed payment transactions is given, for instance, that in Internet banking all information on the payment account is made available online.

(25) In single payment transactions only the essential information should always be given on the payment service provider's own initiative. As the payer is usually present when he gives the payment order, it is not necessary to require that information should in every case be provided on paper or on another durable medium. The payment service provider may give information orally over the counter or make it otherwise easily accessible, for example by keeping the conditions on a notice board on the premises. Information should also be given on where other more detailed information is available (e.g. the address of the website). However, if the consumer so requests, the essential information should be given on paper or on another durable medium.

(26) This Directive should provide for the consumer's right to receive relevant information free of charge before he is bound by any payment service contract. The consumer should also be able to request prior information as well as the framework contract, on paper, free of charge at any time during the contractual relationship, so as to enable him to compare payment service providers' services and their conditions and in case of any dispute verify his contractual rights and obligations. Those provisions should be compatible with Directive 2002/65/EC. The explicit provisions on free information in this Directive should not have the effect of allowing charges to be imposed for the provision of information to consumers under other applicable Directives.

(27) The way in which the required information is to be given by the payment service provider to the payment service user should take into account the needs of the latter as well as practical technical aspects and cost-efficiency depending on the situation with regard to the agreement in the respective payment service contract. Thus, this Directive should distinguish between two ways in which information is to be given by the payment service provider:

Figur 2.7

either the information should be provided, i.e. actively communicated by the payment service provider at the appropriate time as required by this Directive without further prompting by the payment service user, or the information should be made available to the payment service user, taking into account any request he may have for further information. In the latter case, the payment service user should take some active steps in order to obtain the information, such as requesting it explicitly from the payment service provider, logging into bank account mail box or inserting a bank card into printer for account statements. For such purposes the payment service provider should ensure that access to the information is possible and that the information is available to the payment service user.

(28) In addition, the consumer should receive basic information on executed payment transactions for no additional charge. In the case of a single payment transaction the payment service provider should not charge separately for this information. Similarly, the subsequent monthly information on payment transactions under a framework contract should be given free of charge. However, taking into account the importance of transparency in pricing and differing customer needs, the parties should be able to agree on charges for more frequent or additional information. In order to take into account different national practices, Member States should be allowed to set rules requiring that monthly paper-based statements of payment accounts are always to be given free of charge.

(29) In order to facilitate customer mobility, it should be possible for consumers to terminate a framework contract after the expiry of a year without incurring charges. For consumers, the period of notice agreed should be no longer than a month, and for payment service providers no shorter than two months. This Directive should be without prejudice to the payment service provider's obligation to terminate the payment service contract in exceptional circumstances under other relevant Community or national legislation, such as legislation on money laundering and terrorist financing, any action targeting the freezing of funds, or any specific measure linked to the prevention and investigation of crimes.

(30) Low value payment instruments should be a cheap and easy-to-use alternative in the case of low-priced goods and services and should not be overburdened by excessive requirements. The relevant information requirements and rules on their execution should therefore be limited to essential information, taking also into account technical capabilities that can justifiably be expected from instruments dedicated to low value payments. Despite the lighter regime payment service users should benefit from adequate protection considering the limited risks posed by those payment instruments, especially with regard to prepaid payment instruments.

(31) In order to reduce the risks and consequences of unauthorised or incorrectly executed payment transactions the payment service user should inform the payment service provider as soon as possible about any contestations concerning allegedly unauthorised or incorrectly executed payment transactions provided that the payment service provider has fulfilled his

Figur 2.8

information obligations under this Directive. If the notification deadline is met by the payment service user, he should be able to pursue those claims within the prescription periods pursuant to national law. This Directive should not affect other claims between payment service users and payment service providers.

(32) In order to provide an incentive for the payment service user to notify, without undue delay, his provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a limited amount, unless the payment service user has acted fraudulently or with gross negligence. Moreover, once a user has notified a payment service provider that his payment instrument may have been compromised, the user should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to the payment service providers' responsibility for technical security of their own products.

(33 In order to assess possible negligence by the payment service user, account should be taken of all the circumstances. The evidence and degree of alleged negligence should be evaluated according to national law. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered null and void.

(34) However, Member States should be able to establish less stringent rules than mentioned above in order to maintain existing levels of consumer protection and promote trust in the safe usage of electronic payment instruments. The fact that different payment instruments involve different risks should be taken into account accordingly thus promoting the issuance of safer instruments. Member States should be allowed to reduce or completely waive the payer's liability except where the payer has acted fraudulently.

(35) Provisions should be made for the allocation of losses in the case of unauthorised payment transactions. Different provisions may apply to payment service users who are not consumers, since such users are normally in a better position to assess the risk of fraud and take countervailing measures.

(36) This Directive should lay down rules for a refund to protect the consumer when the executed payment transaction exceeds the amount which could reasonably have been expected. Payment service providers should be able to provide even more favourable terms to their customers and, for example, refund any disputed payment transactions. In cases where the user makes a claim for the refund of a payment transaction refund rights should affect neither the liability of the payer vis-à-vis the payee from the underlying relationship, e.g. for goods or services ordered, consumed or legitimately charged, nor the users rights with regard to revocation of a payment order.

(37) For financial planning and the fulfilment of payment obligations in due time, consumers and enterprises need to have certainty on the length of time that the execution of a payment order takes. Therefore, this Directive should introduce

Figur 2.9

a point in time at which rights and obligations take effect, namely, when the payment service provider receives the payment order, including when he has had the opportunity to receive it through the means of communication agreed in the payment service contract, notwithstanding any prior involvement in the process leading up to the creation and transmission of the payment order, e.g. security and availability of funds checks, information on the use of the personal identity number or issuance of a payment promise. Furthermore, the receipt of a payment order should occur when the payer's payment service provider receives the payment order to be debited from the payer's account. The day or moment in time when a payee transmits to his service provider payment orders for the collection e.g. of card payment or of direct debits or when the payee is granted a pre-financing on the related amounts by his payment service provider (by way of a contingent credit to his account) should have no relevance in this respect. Users should be able to rely on the proper execution of a complete and valid payment order if the payment service provider has no contractual or statutory ground for refusal. If the payment service provider refuses a payment order, the refusal and the reason therefor should be communicated to the payment service user at the earliest opportunity subject to the requirements of Community and national law.

(38) In view of the speed with which modern fully automated payment systems process payment transactions, which means that after a certain point in time payment orders cannot be revoked without high manual intervention costs, it is necessary to specify a clear deadline for payment revocations. However, depending on the type of the payment service and the payment order, the point in time may be varied by agreement between the parties. Revocation, in this context, is applicable only to the relationship between a payment service user and payment service provider, thus being without prejudice to the irrevocability and finality of payment transactions in payment systems.

(39) Such irrevocability should not affect a payment service provider's right or obligation under the laws of some Member States, based on the payer's framework contract or national laws, regulations, administrative provisions or guidelines, to reimburse the payer with the amount of the executed payment transaction in the event of a dispute between the payer and the payee. Such reimbursement should be considered to be a new payment order. Except for those cases, legal disputes arising within the relationship underlying the payment order should be settled only between the payer and the payee.

(40) It is essential, for the fully integrated straight-through processing of payments and for legal certainty with respect to the fulfilment of any underlying obligation between payment service users, that the full amount transferred by the payer should be credited to the account of the payee. Accordingly, it should not be possible for any of the intermediaries involved in the execution of payment transactions to make deductions from the amount transferred. However, it should be possible for the payee to enter into an agreement with his payment service provider under which the latter may deduct his own charges. Nevertheless, in order to enable the payee to verify that the amount due is correctly paid, subsequent information provided on the payment

Figur 2.10

transaction should indicate not only the full amount of funds transferred but also the amount of any charges.

(41) With regard to charges, experience has shown that the sharing of charges between a payer and a payee is the most efficient system since it facilitates the straight-through processing of payments. Provision should therefore be made for charges to be levied, in the normal course, directly on the payer and the payee by their respective payment service providers. However, that should apply only where the payment transaction does not require currency exchange. The amount of any charges levied may also be zero as the provisions of this Directive do not affect the practice whereby the payment service provider does not charge consumers for crediting their accounts. Similarly, depending on the contract terms, a payment service provider may charge only the payee (merchant) for the use of the payment service, which has the effect that no charges are imposed on the payer. The charging of the payment systems may be in the form of a subscription fee. The provisions on the amount transferred or any charges levied have no direct impact on pricing between payment service providers or any intermediaries.

(42) In order to promote transparency and competition, the payment service provider should not prevent the payee from requesting a charge from the payer for using a specific payment instrument. While the payee should be free to levy charges for the use of a certain payment instrument, Member States may decide whether they forbid or limit any such practice where, in their view, this may be warranted in view of abusive pricing or pricing which may have a negative impact on the use of a certain payment instrument taking into account the need to encourage competition and the use of efficient payment instruments.

(43) In order to improve the efficiency of payments throughout the Community, all payment orders initiated by the payer and denominated in euro or the currency of a Member State outside the euro area, including credit transfers and money remittances, should be subject to a maximum one-day execution time. For all other payments, such as payments initiated by or through a payee, including direct debits and card payments, in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, the same one-day execution time should apply. The periods above could be extended by an additional business day, if a payment order is given on paper. This allows the continued provision of payment services for those consumers who are used to paper documents only. When a direct debit scheme is used the payee's payment service provider should transmit the collection order within the time limits agreed between the payee and his payment service provider, enabling settlement at the agreed due date. In view of the fact that national payment infrastructures are often highly efficient and in order to prevent any deterioration in current service levels, Member States should be allowed to maintain or set rules specifying an execution time shorter than one business day, where appropriate.

Figur 2.11

(44) The provisions on execution for the full amount and execution time should constitute good practice where one of the service providers is not located in the Community.

(45) It is essential for payment service users to know the real costs and charges of payment services in order to make their choice. Accordingly, the use of non-transparent pricing methods should not be allowed, since it is commonly accepted that those methods make it extremely difficult for users to establish the real price of the payment service. Specifically, the use of value dating to the disadvantage of the user should not be permitted.

(46) The smooth and efficient functioning of the payment system depends on the user being able to rely on the payment service provider executing the payment transaction correctly and within the agreed time. Usually, the provider is in the position to assess the risks involved in the payment transaction. It is the provider that provides the payments system, makes arrangements to recall misplaced or wrongly allocated funds and decides in most cases on the intermediaries involved in the execution of a payment transaction. In view of all those considerations, it is entirely appropriate, except under abnormal and unforeseeable circumstances, to impose liability on the payment service provider in respect of execution of a payment transaction accepted from the user, except for the payee's payment service provider's acts and omissions for whose selection solely the payee is responsible. However, in order not to leave the payer unprotected in unlikely constellations where it may remain open (non liquet) whether the payment amount was duly received by the payee's payment service provider or not, the corresponding burden of proof should lie upon the payer's payment service provider. As a rule, it can be expected that the intermediary institution, usually a "neutral" body like a central bank or a clearing house, transferring the payment amount from the sending to the receiving payment service provider will store the account data and be able to furnish the latter whenever this may be necessary. Whenever the payment amount has been credited to the receiving payment service provider's account, the payee should immediately have a claim against his payment service provider for credit to his account.

(47) The payer's payment service provider should assume liability for correct payment execution, including, in particular the full amount of the payment transaction and execution time, and full responsibility for any failure by other parties in the payment chain up to the account of the payee. As a result of that liability the payment service provider of the payer should, where the full amount is not credited to the payee's payment service provider, correct the payment transaction or without undue delay refund to the payer the relevant amount of that transaction, without prejudice to any other claims which may be made in accordance with national law. This Directive should concern only contractual obligations and responsibilities between the payment service user and his payment service provider. However, the proper functioning of credit transfers and other payment services requires that payment service providers and their intermediaries, such as processors, have contracts where their mutual rights and obligations are agreed upon. Questions related to liabilities form an essential part of these uniform contracts. To ensure the reliability among

Figur 2.12

payment service providers and intermediaries taking part in a payment transaction, legal certainty is necessary to the effect that a non-responsible payment service provider is compensated for losses incurred or sums paid under the provisions of this Directive relating to liability. Further rights and details of content of recourse and how to handle claims towards the payment service provider or intermediary attributable to a defective payment transaction should be left to be defined by contractual arrangements.

(48) It should be possible for the payment service provider to specify unambiguously the information required to execute a payment order correctly. On the other hand, however, in order to avoid fragmentation and jeopardising the setting-up of integrated payment systems in the Community, Member States should not be allowed to require a particular identifier to be used for payment transactions. However, this should not prevent Member States from requiring the payment service provider of the payer to act in due diligence and verify, where technically possible and without requiring manual intervention, the coherence of the unique identifier, and where the unique identifier is found to be incoherent, to refuse the payment order and inform the payer thereof. The liability of the payment service provider should be limited to the correct execution of the payment transaction in accordance with the payment order of the payment service user.

(49) In order to facilitate effective fraud prevention and combat payment fraud across the Community, provision should be made for the efficient exchange of data between payment service providers who should be allowed to collect, process and exchange personal data relating to persons involved in payment fraud. All those activities should be conducted in compliance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data .

(50) It is necessary to ensure the effective enforcement of the provisions of national law adopted pursuant to this Directive. Appropriate procedures should therefore be established by means of which it will be possible to pursue complaints against payment service providers which do not comply with those provisions and to ensure that, where appropriate, effective, proportionate and dissuasive penalties are imposed.

(51) Without prejudice to the right of customers to bring action in the courts, Member States should ensure an easily accessible and cost-sensitive out-of-court resolution of conflicts between payment service providers and consumers arising from the rights and obligations set out in this Directive. Article 5(2) of the Rome Convention on the law applicable to contractual obligations ensures that the protection afforded to consumers by the mandatory rules of the law of the country in which they have their habitual residence may not be undermined by any contractual terms on law applicable.

(52) Member States should determine whether the competent authorities designated for granting authorisation to payment institutions might also be the competent authorities with regard to out-of-court complaint and redress procedures.

Figur 2.13

(53) This Directive should be without prejudice to provisions of national law relating to the consequences as regards liability of inaccuracy in the expression or transmission of a statement.

(54) Since it is necessary to review the efficient functioning of this Directive and to monitor progress on the establishment of a single payment market, the Commission should be required to produce a report three years after the end of the transposition period of this Directive. With regard to the global integration of financial services and harmonised consumer protection also beyond the efficient functioning of this Directive focal points of the review should be the possible need to expand the scope of application with regard to non-EU currencies and to payment transactions where only one payment service provider concerned is located in the Community.

(55) Since the provisions of this Directive replace those of Directive 97/5/EC, that Directive should be repealed.

(56) It is necessary to lay down more detailed rules concerning the fraudulent use of payment cards, an area currently covered by Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts and Directive 2002/65/EC. Those Directives should therefore be amended accordingly.

(57) Since, pursuant to Directive 2006/48/EC, financial institutions are not subject to the rules applicable to credit institutions, they should be made subject to the same requirements as payment institutions so that they are able to provide payment services throughout the Community. Directive 2006/48/EC should therefore be amended accordingly.

(58) Since money remittance is defined in this Directive as a payment service which requires an authorisation for a payment institution or a registration for some natural or legal persons benefiting from a waiver clause under certain circumstances specified in the provisions of this Directive, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing should be amended accordingly.

(59) In the interests of legal certainty, it is appropriate to make transitional arrangements in accordance with which persons who have commenced the activities of payment institutions in accordance with the national law in force before the entry into force of this Directive may continue those activities within the Member State concerned for a specified period.

(60) Since the objective of this Directive, namely, the establishment of a single market in payment services, cannot be sufficiently achieved by the Member States because it requires the harmonisation of a multitude of different rules currently existing in the legal systems of the various Member States and can therefore be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

Figur 2.14

(61) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission.

(62) In particular, the Commission should be empowered to adopt implementing provisions in order to take account of technological and market developments. Since those measures are of general scope and are designed to amend non-essential elements of this Directive, they must be adopted in accordance with the regulatory procedure with scrutiny provided for in Article 5a of Decision 1999/468/EC.

(63) In accordance with point 34 of the Interinstitutional Agreement on better law-making, Member States are encouraged to draw up, for themselves and in the interest of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public,

HAVE ADOPTED THIS DIRECTIVE:

TITLE I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter

1. This Directive lays down the rules in accordance with which Member States shall distinguish the following six categories of payment service provider:

(a) credit institutions within the meaning of Article 4(1)(a) of Directive 2006/48/EC;

(b) electronic money institutions within the meaning of Article 1(3)(a) of Directive 2000/46/EC;

(c) post office giro institutions which are entitled under national law to provide payment services;

(d) payment institutions within the meaning of this Directive;

(e) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities;

(f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

2. This Directive also lays down rules concerning transparency of conditions and information requirements for payment services, and the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services as a regular occupation or business activity.

Figur 2.15

Article 2

Scope

1. This Directive shall apply to payment services provided within the Community. However, with the exception of Article 73, Titles III and IV shall apply only where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located in the Community.

2. Titles III and IV shall apply to payment services made in euro or the currency of a Member State outside the euro area.

3. Member States may waive the application of all or part of the provisions of this Directive to the institutions referred to in Article 2 of Directive 2006/48/EC, with the exception of those referred to in the first and second indent of that article.

Article 3

Negative scope

This Directive shall apply to none of the following:

(a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;

(b) payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee;

(c) professional physical transport of banknotes and coins, including their collection, processing and delivery;

(d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;

(e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;

(f) money exchange business, that is to say, cash-to-cash operations, where the funds are not held on a payment account;

(g) payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee:

(i) paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

Figur 2.16

(ii) paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(iv) paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(v) paper-based vouchers;

(vi) paper-based traveller's cheques; or

(vii) paper-based postal money orders as defined by the Universal Postal Union;

(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to Article 28;

(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services;

(k) services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;

(l) payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;

(m) payment transactions carried out between payment service providers, their agents or branches for their own account;

Figur 2.17

(n) payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group; or

(o) services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex.

Article 4

Definitions

For the purposes of this Directive, the following definitions shall apply:

1. "home Member State" means either of the following:

   (i) the Member State in which the registered office of the payment service provider is situated; or

   (ii) if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated;

2. "host Member State" means the Member State other than the home Member State in which a payment service provider has an agent or a branch or provides payment services;

3. "payment service" means any business activity listed in the Annex;

4. "payment institution" means a legal person that has been granted authorisation in accordance with Article 10 to provide and execute payment services throughout the Community;

5. "payment transaction" means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

6. "payment system" means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions;

7. "payer" means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

8. "payee" means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

9. "payment service provider" means bodies referred to in Article 1(1) and legal and natural persons benefiting from the waiver under Article 26;

Figur 2.18

10. "payment service user" means a natural or legal person making use of a payment service in the capacity of either payer or payee, or both;

11. "consumer" means a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his trade, business or profession;

12. "framework contract" means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;

13. "money remittance" means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;

14. "payment account" means an account held in the name of one or more payment service users which is used for the execution of payment transactions;

15. "funds" means banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC;

16. "payment order" means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;

17. "value date" means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;

18. "reference exchange rate" means the exchange rate which is used as the basis to calculate any currency exchange and which is made available by the payment service provider or comes from a publicly available source;

19. "authentication" means a procedure which allows the payment service provider to verify the use of a specific payment instrument, including its personalised security features;

20. "reference interest rate" means the interest rate which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract;

21. "unique identifier" means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously the other payment service user and/or his payment account for a payment transaction;

22. "agent" means a natural or legal person which acts on behalf of a payment institution in providing payment services;

Figur 2.19

23. "payment instrument" means any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order;

24. "means of distance communication" refers to any means which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract;

25. "durable medium" means any instrument which enables the payment service user to store information addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;

26. "micro-enterprise" means an enterprise, which at the time of conclusion of the payment service contract, is an enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC;

27. "business day" means a day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction;

28. "direct debit" means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider;

29. "branch" means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out directly some or all of the transactions inherent in the business of a payment institution; all the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch;

30. "group" means a group of undertakings, which consists of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries have a holding as well as undertakings linked to each other by a relationship referred to in Article 12(1) of Directive 83/349/EEC.

Figur 2.20

CHAPTER 2

Authorisation of payment transactions

Article 54

Consent and withdrawal of consent

1. Member States shall ensure that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and his payment service provider, after the execution of the payment transaction.

2. Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and his payment service provider.

In the absence of such consent, a payment transaction shall be considered to be unauthorised.

3. Consent may be withdrawn by the payer at any time, but no later than the point in time of irrevocability under Article 66. Consent to execute a series of payment transactions may also be withdrawn with the effect that any future payment transaction is to be considered as unauthorised.

4. The procedure for giving consent shall be agreed between the payer and the payment service provider.

Article 55

Limits of the use of the payment instrument

1. In cases where a specific payment instrument is used for the purposes of giving consent, the payer and his payment service provider may agree on spending limits for payment transactions executed through that payment instrument.

2. If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons related to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil his liability to pay.

3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible, before the payment instrument is blocked and at the latest immediately thereafter, unless giving such information would compromise objectively justified security reasons or is prohibited by other relevant Community or national legislation.

4. The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.

Figur 2.21

Article 56

Obligations of the payment service user in relation to payment instruments

1. The payment service user entitled to use a payment instrument shall have the following obligations:

(a) to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument; and

(b) to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use.

2. For the purposes of paragraph 1(a), the payment service user shall, in particular, as soon as he receives a payment instrument, take all reasonable steps to keep its personalised security features safe.

Article 57

Obligations of the payment service provider in relation to payment instruments

1. The payment service provider issuing a payment instrument shall have the following obligations:

(a) to make sure that the personalised security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 56;

(b) to refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;

(c) to ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 56(1)(b) or request unblocking pursuant to Article 55(4); on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that he made such notification; and

(d) to prevent all use of the payment instrument once notification pursuant to Article 56(1)(b) has been made.

2. The payment service provider shall bear the risk of sending a payment instrument to the payer or of sending any personalised security features of it.

Figur 2.22

Article 58

Notification of unauthorised or incorrectly executed payment transactions

The payment service user shall obtain rectification from the payment service provider only if he notifies his payment service provider without undue delay on becoming aware of any unauthorised or incorrectly executed payment transactions giving rise to a claim, including that under Article 75, and no later than 13 months after the debit date, unless, where applicable, the payment service provider has failed to provide or make available the information on that payment transaction in accordance with Title III.

Article 59

Evidence on authentication and execution of payment transactions

1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.

2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.

Article 60

Payment service provider's liability for unauthorised payment transactions

1. Member States shall ensure that, without prejudice to Article 58, in the case of an unauthorised payment transaction, the payer's payment service provider refunds to the payer immediately the amount of the unauthorised payment transaction and, where applicable, restores the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

2. Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and his payment service provider.

Article 61

Payer's liability for unauthorised payment transactions

1. By way of derogation from Article 60 the payer shall bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment instrument or, if the payer has failed to keep the

Figur 2.23

personalised security features safe, from the misappropriation of a payment instrument.

2. The payer shall bear all the losses relating to any unauthorised payment transactions if he incurred them by acting fraudulently or by failing to fulfil one or more of his obligations under Article 56 with intent or gross negligence. In such cases, the maximum amount referred to in paragraph 1 of this Article shall not apply.

3. In cases where the payer has neither acted fraudulently nor with intent failed to fulfil his obligations under Article 56, Member States may reduce the liability referred to in paragraphs 1 and 2 of this Article, taking into account, in particular, the nature of the personalised security features of the payment instrument and the circumstances under which it was lost, stolen or misappropriated.

4. The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with Article 56(1)(b), except where he has acted fraudulently.

5. If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under Article 57(1)(c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where he has acted fraudulently.

Article 62

Refunds for payment transactions initiated by or through a payee

1. Member States shall ensure that a payer is entitled to a refund from his payment service provider of an authorised payment transaction initiated by or through a payee which has already been executed, if the following conditions are met:

(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made; and

(b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account his previous spending pattern, the conditions in his framework contract and relevant circumstances of the case.

At the payment service provider's request, the payer shall provide factual elements relating to such conditions.

The refund consists of the full amount of the executed payment transaction.

For direct debits the payer and his payment service provider may agree in the framework contract that the payer is entitled to a refund from his payment service provider even though the conditions for refund in the first subparagraph are not met.

2. However, for the purposes of point (b) of the first subparagraph of paragraph 1, the payer may not rely on currency exchange reasons if the reference exchange rate

Figur 2.24

agreed with his payment service provider in accordance with Articles 37(1)(d) and 42(3)(b) was applied.

3. It may be agreed in the framework contract between the payer and the payment service provider that the payer has no right to a refund where he has given his consent to execute the payment transaction directly to his payment service provider and, where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least four weeks before the due date by the payment service provider or by the payee.

Article 63

Requests for refunds for payment transactions initiated by or through a payee

1. Member States shall ensure that the payer can request the refund referred to in Article 62 of an authorised payment transaction initiated by or through a payee for a period of eight weeks from the date on which the funds were debited.

2. Within ten business days of receiving a request for a refund, the payment service provider shall either refund the full amount of the payment transaction or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter in accordance with Articles 80 to 83 if he does not accept the justification provided.

The payment service provider's right under the first subparagraph to refuse the refund shall not apply in the case set out in the fourth subparagraph of Article 62(1).

CHAPTER 3

Execution of payment transactions

Section 1

Payment orders and amounts transferred

Article 64

Receipt of payment orders

1. Member States shall ensure that the point in time of receipt is the time when the payment order transmitted directly by the payer or indirectly by or through a payee is received by the payer's payment service provider. If the point in time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.

Figur 2.25

2. If the payment service user initiating a payment order and his payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has set funds at his payment service provider's disposal, the point in time of receipt for the purposes of Article 69 is deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.

Article 65

Refusal of payment orders

1. Where the payment service provider refuses to execute a payment order, the refusal and, if possible, the reasons for it and the procedure for correcting any factual mistakes that led to the refusal shall be notified to the payment service user, unless prohibited by other relevant Community or national legislation.

The payment service provider shall provide or make available the notification in an agreed manner at the earliest opportunity, and in any case, within the periods specified in Article 69.

The framework contract may include a condition that the payment service provider may charge for such a notification if the refusal is objectively justified.

2. In cases where all the conditions set out in the payer's framework contract are met, the payer's payment service provider shall not refuse to execute an authorised payment order irrespective of whether the payment order is initiated by a payer or by or through a payee, unless prohibited by other relevant Community or national legislation.

3. For the purposes of Articles 69 and 75 a payment order of which execution has been refused shall be deemed not to have been received.

Article 66

Irrevocability of a payment order

1. Member States shall ensure that the payment service user may not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in this Article.

2. Where the payment transaction is initiated by or through the payee, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee.

3. However, in the case of a direct debit and without prejudice to refund rights the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds.

Figur 2.26

4. In the case referred to in Article 64(2) the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.

5. After the time limits specified in paragraphs 1 to 4, the payment order may be revoked only if agreed between the payment service user and his payment service provider. In the case referred to in paragraphs 2 and 3, the payee's agreement shall also be required. If agreed in the framework contract, the payment service provider may charge for revocation.

Article 67

Amounts transferred and amounts received

1. Member States shall require the payment service provider of the payer, the payment service provider of the payee and any intermediaries of the payment service providers to transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.

2. However, the payee and his payment service provider may agree that the payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.

3. If any charges other than those referred to in paragraph 2 are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. In cases where the payment transaction is initiated by or through the payee, his payment service provider shall ensure that the full amount of the payment transaction is received by the payee.

Section 2

Execution time and value date

Article 68

Scope

1. This Section shall apply to:

(a) payment transactions in euro;

(b) national payment transactions in the currency of the Member State outside the euro area concerned; and

(c) payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside

Figur 2.27

the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro.

2. This Section shall apply to other payment transactions, unless otherwise agreed between the payment service user and his payment service provider, with the exception of Article 73, which is not at the disposal of the parties. However, when the payment service user and his payment service provider agree on a longer period than those laid down in Article 69, for intra-Community payment transactions such period shall not exceed 4 business days following the point in time of receipt in accordance with Article 64.

Article 69

Payment transactions to a payment account

1. Member States shall require the payer's payment service provider to ensure that, after the point in time of receipt in accordance with Article 64, the amount of the payment transaction is credited to the payee's payment service provider's account at the latest by the end of the next business day. Until 1 January 2012, a payer and his payment service provider may agree on a period no longer than three business days. These periods may be extended by a further business day for paper-initiated payment transactions.

2. Member States shall require the payment service provider of the payee to value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with Article 73.

3. Member States shall require the payee's payment service provider to transmit a payment order initiated by or through the payee to the payer's payment service provider within the time limits agreed between the payee and his payment service provider, enabling settlement, as far as direct debit is concerned, on the agreed due date.

Article 70

Absence of payee's payment account with the payment service provider

Where the payee does not have a payment account with the payment service provider, the funds shall be made available to the payee by the payment service provider who receives the funds for the payee within the period specified in Article 69.

Article 71

Cash placed on a payment account

Where a consumer places cash on a payment account with that payment service provider in the currency of that payment account, the payment service provider shall

Figur 2.28

ensure that the amount is made available and value dated immediately after the point of time of the receipt of the funds. Where the payment service user is not a consumer, the amount shall be made available and value dated at the latest on the next business day after the receipt of the funds.

Article 72

National payment transactions

For national payment transactions, Member States may provide for shorter maximum execution times than those provided for in this Section.

Article 73

Value date and availability of funds

1. Member States shall ensure that the credit value date for the payee's payment account is no later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account.

The payment service provider of the payee shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account.

2. Member States shall ensure that the debit value date for the payer's payment account is no earlier than the point in time at which the amount of the payment transaction is debited to that payment account.

Section 3

Liability

Article 74

Incorrect unique identifiers

1. If a payment order is executed in accordance with the unique identifier, the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.

2. If the unique identifier provided by the payment service user is incorrect, the payment service provider shall not be liable under Article 75 for non-execution or defective execution of the payment transaction.

However the payer's payment service provider shall make reasonable efforts to recover the funds involved in the payment transaction.

Figur 2.29

If agreed in the framework contract, the payment service provider may charge the payment service user for recovery.

3. If the payment service user provides information additional to that specified in Articles 37(1)(a) or 42(2)(b), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.

Article 75

Non-execution or defective execution

1. Where a payment order is initiated by the payer, his payment service provider shall, without prejudice to Article 58, Article 74(2) and (3), and Article 78, be liable to the payer for correct execution of the payment transaction, unless he can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 69(1), in which case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.

Where the payer's payment service provider is liable under the first subparagraph, he shall without undue delay refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

Where the payee's payment service provider is liable under the first subparagraph, he shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account.

In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by the payer, his payment service provider shall regardless of liability under this paragraph, on request, make immediate efforts to trace the payment transaction and notify the payer of the outcome.

2. Where a payment order is initiated by or through the payee, his payment service provider shall, without prejudice to Article 58, Article 74(2) and (3), and Article 78, be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with Article 69(3). Where the payee's payment service provider is liable under this subparagraph, he shall immediately re-transmit the payment order in question to the payment service provider of the payer.

In addition, the payment service provider of the payee shall, without prejudice to Article 58, Article 74(2) and (3), and Article 78, be liable to the payee for handling the payment transaction in accordance with its obligations under Article 73. Where the payee's payment service provider is liable under this subparagraph, he shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account.

Figur 2.30

In the case of a non-executed or defectively executed payment transaction for which the payee's payment service provider is not liable under the first and second subparagraphs, the payer's payment service provider shall be liable to the payer. Where the payer's payment service provider is so liable he shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by or through the payee, his payment service provider shall, regardless of liability under this paragraph, on request, make immediate efforts to trace the payment transaction and notify the payee of the outcome.

3. In addition, payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution or defective execution of the payment transaction.

Article 76

Additional financial compensation

Any financial compensation additional to that provided for under this Section may be determined in accordance with the law applicable to the contract concluded between the payment service user and his payment service provider.

Article 77

Right of recourse

1. Where the liability of a payment service provider under Article 75 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Article 75.

2. Further financial compensation may be determined in accordance with agreements between payment service providers and/or intermediaries and the law applicable to the agreement concluded between them.

Article 78

No liability

Liability under Chapter 2 and 3 shall not apply in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by national or Community legislation.

Figur 2.31

TITLE VI

FINAL PROVISIONS

Article 86

Full harmonisation

1. Without prejudice to Article 30(2), Article 33, Article 34(2), Article 45(6), Article 47(3), Article 48(3), Article 51(2), Article 52(3), Article 53(2), Article 61(3), and Articles 72 and 88 insofar as this Directive contains harmonised provisions, Member States shall not maintain or introduce provisions other than those laid down in this Directive.

2. Where a Member State makes use of any of the options referred to in paragraph 1, it shall inform the Commission thereof as well as of any subsequent changes. The Commission shall make the information public on a web-site or other easily accessible means.

3. Member States shall ensure that payment service providers do not derogate, to the detriment of payment service users, from the provisions of national law implementing or corresponding to provisions of this Directive except where explicitly provided for therein.

However, payment service providers may decide to grant more favourable terms to payment service users.

Article 87

Review

No later than 1 November 2012, the Commission shall present to the European Parliament, the Council, the European Economic and Social Committee and the European Central Bank a report on the implementation and impact of this Directive, in particular on:

- the possible need to extend the scope of the Directive to payment transactions in all currencies and to payment transactions where only one of the payment service providers is located in the Community,
- the application of Articles 6, 8 and 9 concerning prudential requirements for payment institutions, in particular as regards own funds requirements and safeguarding requirements (ringfencing),
- the possible impact of the granting of credit by payment institutions related to payments services, as set out in Article 16(3),
- the possible impact of the authorisation requirements of payment institutions on competition between payment institutions and other payment service

Figur 2.32

providers as well as on barriers to market entry by new payment service providers,

- the application of Articles 34 and 53 and the possible need to revise the scope of this Directive with respect to low value payment instruments and electronic money, and
- the application and functioning of Articles 69 and 75 for all kinds of payment instruments,

accompanied, where appropriate, by a proposal for its revision.

Article 94

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 1 November 2009. They shall forthwith inform the Commission thereof.

When they are adopted by Member States, those measures shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 95

Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 96

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 13 November 2007.

For the European Parliament	*For the Council*
The President	*The President*
H.-G. Pöttering	M. Lobo Antunes

Figur 2.33

Vedlegg 3

Utdrag av lov om finansavtaler og finansoppdrag (finansavtaleloven) av 25. juni 1999 nr. 46

Kapittel 1. Alminnelige regler

§ 1. *Virkeområde*

(1) Denne loven gjelder for avtaler og oppdrag om finansielle tjenester med finansinstitusjoner eller lignende institusjoner hvis ikke annet er fastsatt i eller i medhold av lov.

(2) Med lignende institusjoner menes i denne loven

a) statsbank
b) finansmeglerforetak
c) finansagent eller finansrådgiver
d) samvirkeforetak
e) pensjonsinnretning som omfattes av forsikringsloven.
f) institusjon som loven gjelder for etter forskrift med hjemmel i fjerde ledd bokstav a.

(3) Loven gjelder ikke mellom to parter som begge er finansinstitusjoner eller lignende institusjoner og opptrer i denne egenskap.

(4) For lån der långiveren er en kommune eller en fylkeskommune, gjelder kapittel 3 i loven. Kapittel 4 i loven gjelder for kausjoner for slike lån.

(5) Kongen kan gi forskrifter om lovens virkeområde, herunder om at

a) loven skal gjelde helt eller delvis for andre enn institusjoner nevnt i første ledd
b) enkelte bestemmelser i loven ikke skal gjelde for visse institusjoner.

§ 2. *Ufravikelighet*

(1) Loven kan ikke fravikes ved avtale til skade for en forbruker. Med forbruker menes en fysisk person når avtalens formål for denne ikke hovedsakelig er knyttet til næringsvirksomhet.

(2) Når institusjonens kunde ikke er en forbruker, viker loven for avtale, etablert praksis mellom partene eller annen sedvane som anses bindende mellom partene. Bestemmelsene i §§ 14, 16, 20 første punktum, 21 tredje ledd, 27, 28, 48 og 61 samt kapitlene 5 og 6 kan likevel ikke fravikes til skade for kunden. Bestemmelsene i kapittel 3 kan ikke fravikes til skade for låntakeren dersom låntakeren er en fysisk person, og lån eller lignende kreditt er sikret ved pant i et formuesgode som tilhører låntakeren uten at godet hovedsakelig er knyttet til låntakerens næringsvirksomhet.

(3) En bestemmelse som ikke kan fravikes til skade for en forbruker, kan ikke settes til side ved avtale om at fremmed rett skal anvendes.

Figur 3.1

§ 3. *Anvendelse av norsk rett*

Har en forbruker bosatt i Norge inngått avtale med en institusjon hjemmehørende i annet land, skal norsk rett gjelde for avtalen dersom

a) institusjonen har gitt forbrukeren tilbud eller markedsført tjenesten her i riket, og forbrukeren her har gjort det som er nødvendig for at avtalen skal kunne inngås

b) institusjonen eller en kommisjonær, agent eller annen representant for denne eller en megler her i riket har mottatt forbrukerens tilbud, aksept eller bestilling, eller

c) avtalen er inngått av forbrukeren etter reise til utlandet i forbindelse med erverv av fast eiendom eller løsøregjenstand eller finansiering av ervervet, og reisen er arrangert av institusjonen, eller av selger i forståelse med institusjonen.

§ 4. *Nemndsbehandling*

(1) Gjennom avtale mellom en finansinstitusjon eller en lignende institusjon eller en organisasjon for slike institusjoner på den ene siden, og på den annen side Forbrukerrådet eller en annen organisasjon som representerer institusjonenes kunder, kan det opprettes en eller flere nemnder for behandling av tvister om finansavtaler.

(2) Partene kan forelegge avtalen for Kongen til godkjenning. Har Kongen godkjent nemndas vedtekter, gjelder bestemmelsene i tredje til femte ledd.

(3) Kunden kan kreve nemndsbehandling av enhver tvist hvor nemnda er kompetent, såfremt kunden har saklig interesse i å få nemndas uttalelse i saken. Tvist om urettmessig belastning av konto eller urettmessig bruk av betalingsinstrument, jf. § 37, kan også institusjonen bringe inn for nemnda.

(4) Så lenge en tvist er til behandling i nemnda, kan ikke en part bringe den inn for de alminnelige domstoler. Bestemmelsen i første punktum er likevel ikke til hinder for tvangsfullbyrdelse etter tvangsfullbyrdelsesloven eller midlertidig sikring etter tvisteloven.

(5) En sak som nemnda har realitetsbehandlet, kan bringes direkte inn for tingrett.

§ 5. *Avtale om tvisteløsning*

(1) En finansavtale med en forbruker skal inneholde opplysning om tvisteordning som nevnt i § 4. En forbruker kan ikke fraskrive seg adgangen til å kreve nemndsbehandling.

(2) En forbruker kan ikke på forhånd avtale voldgift. Dersom ikke annet følger av lov, kan en forbruker heller ikke på forhånd vedta annet verneting enn de lovbestemte.

§ 6. *Sletting av pantheftelser m.v.*

(1) Når en fordring er innfridd eller for øvrig bortfalt, skal kreditor sørge for sletting eller frigivelse av pant og annen sikkerhet for fordringen, dersom ikke annet er avtalt i forbindelse med innfrielsen. Kausjonsdokument skal leveres tilbake til kausjonisten.

(2) Gjeldsbrev og annet dokument som har tjent som bevis for långiverens fordring, skal gjøres ugyldig og leveres tilbake til låntakeren.

Figur 3.2

§ 7. *Brudd på andre avtaler*

(1) Institusjonen kan ikke i en finansavtale med en forbruker betinge seg rett til å heve eller si opp avtalen eller til å anse fordring i henhold til avtalen som forfalt, på grunn av at kunden har misligholdt en annen avtale eller fordring.

(2) Hvis kunden overfor institusjonen har handlet klart i strid med redelighet og god tro, har institusjonen slik rett som nevnt i første ledd uten hensyn til om forbehold er inntatt i finansavtalen. Det samme gjelder andre institusjoner i samme konsern dersom dette er saklig begrunnet.

§ 8. *Bruk av elektronisk kommunikasjon og elektroniske medier*

(1) Krav i eller i medhold av denne loven om at opplysninger eller meldinger skal gis skriftlig, er ikke til hinder for bruk av elektronisk kommunikasjon dersom kunden ønsker dette.

(2) Krav i eller i medhold av denne loven om at en avtale skal inngås skriftlig, er ikke til hinder for at avtalen inngås ved hjelp av et elektronisk medium dersom kunden ønsker dette, og

a) avtalens innhold i sin helhet er tilgjengelig for kunden ved avtaleinngåelsen, og

b) det er benyttet en betryggende metode for å autentifisere inngåelsen av en avtale med det angitte innhold.

Kapittel 2. Innskudd og betalingsoppdrag

I. Innledende bestemmelser

§ 9. *Virkeområde*

(1) Dette kapitlet gjelder for avtaler om innskudd og for bruk av innskuddskonto i finansinstitusjoner eller lignende institusjoner som nevnt i § 1 annet ledd. Dersom det er knyttet en kredittordning til en innskuddskonto, gjelder også reglene i kapittel 3.

(2) Bestemmelsene i avsnitt VI gjelder forholdet mellom betaleren og mottakeren ved betalingsoverføringer.

(3) Kongen fastsetter i forskrift særlige regler om betalingsoppdrag til og fra utlandet. EØS-avtalen vedlegg XII nr. 3 (forordning (EF) nr. 2560/2001) om grensekryssende betalinger i euro gjelder som lov med de tilpasninger som følger av vedlegg XII, protokoll 1 til avtalen og avtalen for øvrig. Departementet kan gi forskrift om at disse reglene også gjelder for annen valuta.

(4) Kongen kan i forskrift fastsette særlige regler om innenlandske valutatransaksjoner. § 27 og § 41 annet ledd gjelder bare ved innenlandske valutatransaksjoner dersom det er bestemt i en slik forskrift.

§ 10. *Særlige innskuddsformer*

(1) Bestemmelsene om innskudd i dette kapitlet gjelder ikke for

a) forsikringsavtale

b) pensjonsspareavtale

c) avtale om innskudd i verdipapirfond.

(2) Bestemmelsene om innskudd i dette kapitlet gjelder tilsvarende for innlån

Figur 3.3

til finansinstitusjoner eller lignende institusjoner, med unntak av
a) lån ved ihendehaverobligasjoner og sertifikater
b) ansvarlig lån.

§ 11. *Betalingsoppdrag som ikke skal belastes innskuddskonto*
(1) For betalingsoppdrag som ikke skal belastes innskuddskonto, gjelder bestemmelsene i §§ 12, 13, 14, 28, 29 annet ledd og avsnitt V, VI og VII tilsvarende.
(2) Bestemmelsene i dette kapitlet gjelder ikke for forhåndsbetalte elektroniske kort dersom ikke kortet kan brukes til å disponere en innskuddskonto. Kongen kan i forskrift fastsette særlige regler om forhåndsbetalte elektroniske kort.

§ 12. *Definisjoner*
I dette kapitlet betyr
a) *betalingsoppdrag*: oppdrag om uttak eller overføring av betalingsmidler
b) *betalingsmidler*: pengesedler og mynter (kontanter), samt innskudd og kreditt på konto i en finansinstitusjon eller en lignende institusjon som kan disponeres ved bruk av betalingsinstrumenter
c) *betalingsinstrument*: sjekk, giroblankett, betalingskort eller annet særskilt hjelpemiddel for uttak eller overføring av betalingsmidler
d) *betalingskort*: elektronisk eller manuelt benyttet uttaks-, debet- og kredittkort eller lignende kort for uttak eller overføring av betalingsmidler
e) *virkedag*: hver av ukedagene fra og med mandag til og med fredag med unntak av helligdager og offentlige høytidsdager.

§ 13. *Alminnelige vilkår*
(1) De alminnelige vilkår for innskudd og betalingsoppdrag som en institusjon benytter, skal holdes tilgjengelig for kundene på ekspedisjonsstedene.
(2) Alminnelige vilkår for betalingsoppdrag skal opplyse om høyeste antall virkedager for å gjennomføre betalingsoppdrag.

§ 14. *Avvisning av kunder*
(1) Institusjonen kan ikke uten saklig grunn avslå å ta imot innskudd eller utføre betalingsoppdrag på vanlige vilkår.
(2) Kunden skal underrettes om avslag uten ugrunnet opphold når ikke annet er bestemt i eller i medhold av lov. Underretningen om avslag skal inneholde opplysning om tvisteordning som er etablert etter § 4.

II. Avtalen

§ 15. *Opplysningsplikt m.v.*
(1) Institusjonen skal veilede kunden i valget mellom de ulike typer av innskuddskontoer som den tilbyr.
(2) Før det blir inngått en kontoavtale med en forbruker, skal institusjonen skriftlig opplyse kunden om
a) nominell årlig rente, samt for andre kontoer enn brukskontoer nevnt i § 30 annet ledd annet punktum, representative eksempler på effektiv rente
b) kostnader ved å etablere, ha eller avvikle kontoen, betalingsinstrument knyttet til den eller annen del av kontoforholdet

Figur 3.4

c) kostnader som påløper ved å bruke kontoen og betalingsinstrument knyttet til den
d) regler om hvordan kontoen og betalingsinstrument knyttet til kontoen kan brukes, herunder krav til legitimasjon
e) reklamasjonsplikten som følger av § 37 første ledd
f) begrensninger i kontohaverens adgang til straks å si opp avtalen og til å ta ut midler fra kontoen, jf. §§ 21 første ledd og 24 tredje ledd
g) ansvar og risiko ved bruk av kontoen og for andres urettmessige bruk av den
h) tidspunktet for godskriving av renter, såfremt renter ikke skal godskrives ved årets utgang
i) hvilke regler som gjelder for innskuddsgaranti.

(3) Skriftlig informasjon med opplysninger som nevnt i annet ledd, skal være tilgjengelig for alle kunder. Brosjyrer og lignende markedsføringsmateriell om innskudd og betalingsoppdrag skal alltid inneholde opplysninger som nevnt i annet ledd bokstav a, b, c, f og h.

§ 16. *Kontoavtalen*

(1) Kontoavtalen skal være skriftlig. Den skal inneholde navn og adresse samt fødselsnummer eller organisasjonsnummer på kontohaveren og enhver som skal disponere kontoen. Dersom slikt nummer ikke eksisterer, skal fødselsdato eller annen entydig identifikasjon benyttes.

(2) Kontoavtalen skal inneholde opplysninger som nevnt i § 15 annet ledd bokstav a til i. En kontoavtale med en forbruker skal inneholde opplysning om tvisteordning som er etablert etter § 4. Opplysninger som nevnt i § 15 annet ledd som institusjonen har gitt før avtalen ble inngått, skal i alle tilfeller regnes som en del av kontoavtalen.

(3) Et vilkår som ikke er tatt inn i kontoavtalen, er ikke bindende for kontohaveren med mindre institusjonen godtgjør at vilkåret er vedtatt av kontohaveren.

(4) Institusjonen skal gi kontohaveren et eksemplar av avtalen eller på annen måte gjøre avtalen tilgjengelig for kontohaveren.

(5) Kongen kan gi nærmere regler om krav til innholdet i kontoavtalen og om gjennomføring og avgrensning av opplysningsplikten etter § 15.

§ 17. *Ihendehaverklausul*

Innskuddsbok kan ikke inneholde vilkår om at institusjonen med befriende virkning kan utbetale penger til den som har innskuddsboken i hende (ihendehaverklausul).

§ 18. *Endring av kontoavtalen*

(1) Er partene enige om å endre kontoavtalen, gjelder §§ 15 og 16 tilsvarende så langt de passer.

(2) Institusjonen kan ikke i en kontoavtale med en forbruker forbeholde seg rett til ensidig å endre avtalevilkår til skade for kontohaveren, med unntak av

a) nedsettelse av rentesats
b) økning av gebyrer for å ha eller bruke kontoen eller betalingsinstrument knyttet til denne.

Figur 3.5

(3) Institusjonen kan uten hensyn til om forbehold er tatt inn i kontoavtalen, øke satsene for overtrekksrente og purregebyr ved urettmessig overtrekk.

§ 19. *Varsel om ensidig endring av avtalevilkårene*

(1) Endring av vilkårene i kontoavtalen til kontohaverens skade kan tidligst settes i verk to uker etter at institusjonen har sendt skriftlig varsel til kontohaveren om endringen.

(2) Varsel om endring av rentesatser og gebyrer skal opplyse om

a) hva endringene går ut på

b) kontohaverens rett til å si opp avtalen og få utbetalt innestående på kontoen med tillegg av påløpte renter, og i den forbindelse hvilke regler som gjelder for avviklingsvederlag og forhåndsbetalt periodeavgift.

(3) Varsel om endring kan tas med i kontoutskrift.

(4) For andre typer innskuddskontoer enn brukskonto som nevnt i § 30 annet ledd annet punktum, kan varsel unnlates når saldo på konto utgjør mindre enn kr 1.000 med mindre Kongen i forskrift fastsetter et annet beløp.

§ 20. *Vederlag ved avvikling*

Institusjonen kan bare kreve vederlag (gebyr) for avvikling av kontoforholdet eller deler av dette i den utstrekning dette følger av kontoavtalen. Når kunden er en forbruker, må opplysning om slikt vederlag være gitt på forhånd, jf. § 15 annet ledd bokstav b. Vederlagets størrelse skal ikke overstige antatte kostnader ved avviklingen.

§ 21. *Kontohaverens oppsigelse og heving*

(1) Når ikke annet er avtalt, jf. § 24 tredje ledd, kan kontohaveren si opp kontoavtalen uten forhåndsvarsel for å få avviklet kontoforholdet.

(2) En bestemmelse i kontoavtalen som begrenser kontohaverens rett til å si opp avtalen, kan ikke gjøres gjeldende dersom institusjonen ensidig endrer avtalevilkår til kontohaverens skade, jf. § 18 annet ledd, og kontohaveren sier opp kontoavtalen innen fire uker etter at varsel etter § 19 er sendt til kontohaveren.

(3) Uten hensyn til hva som er avtalt i kontoavtalen, kan kontohaveren heve avtalen dersom det fra institusjonens side foreligger vesentlig brudd på opplysningsplikten eller kontoavtalen. Krav om heving må fremsettes innen rimelig tid etter at kontohaveren ble eller burde ha blitt klar over hevingsgrunnen.

(4) Avsluttes kontoforholdet etter tredje ledd, har kontohaveren rett til å få utbetalt pengene på kontoen med påløpte renter og uten fradrag for vederlag som nevnt i § 20. Det samme gjelder når institusjonen foretar en ikke uvesentlig endring av rente- eller gebyrsatser og kontohaveren sier opp innen slik frist som nevnt i annet ledd. Kontohaveren har i disse tilfeller også rett til å få tilbakebetalt en forholdsmessig del av forhåndsbetalt periodeavgift.

§ 22. *Institusjonens oppsigelse og heving*

(1) Institusjonen kan skriftlig si opp avtalen med minst fire ukers varsel dersom det foreligger saklig grunn og det ikke er avtalt lengre bindingstid. Grunnen til oppsigelsen skal opplyses. § 21 fjerde ledd gjelder tilsvarende.

(2) Institusjonen kan skriftlig heve avtalen ved vesentlig mislighold fra kontohaverens side. Grunnen til hevingen skal opplyses.

Figur 3.6

§ 23. *Konto som ikke brukes*

(1) Er det ikke satt inn eller tatt ut noe på en innskuddskonto i løpet av ti år, skal institusjonen gi melding om kontoen i rekommandert brev til kontohaverens eller arvingenes sist kjente adresse. Meldingen skal opplyse om når foreldelsesfristen etter foreldelsesloven § 4 begynner å løpe, når fristen vil løpe ut, og hva som kreves for å avbryte fristen.

(2) Nødvendige kostnader for å komme i kontakt med kontohaveren eller arvingene etter bestemmelsen i foreldelsesloven § 4 første ledd tredje punktum kan belastes kontoen.

III. Bruk av konto, betalingsoppdrag m.v.

§ 24. *Disponering av konto*

(1) Kontohaveren kan bruke kontoen til innskudd, uttak og betalingsoverføringer i samsvar med kontoavtalen.

(2) Innskudd på brukskonto som nevnt i § 30 annet ledd annet punktum kan disponeres når det er godskrevet kontoen. Innskudd i kontanter på slik konto kan straks heves på institusjonens ekspedisjonssteder.

(3) For andre typer innskuddskontoer enn nevnt i annet ledd kan kontoavtalen fastsette oppsigelsestid og bindingstid for innskudd.

§ 25. *Umyndig kontohaver*

(1) Umyndiges midler som bare kan disponeres av verge eller overformynderi, skal ikke settes inn på konto som den umyndige har rett til å disponere på egen hånd.

(2) Opplysninger som institusjonen etter loven her skal meddele kontohaveren, skal gis verge eller overformynderiet med mindre opplysningene gjelder midler den umyndige har rett til å disponere over på egen hånd.

(3) Har en umyndig kontohaver flere verger, disponerer de kontoen i fellesskap med mindre de skriftlig har gitt melding om noe annet.

§ 26. *Avtale om belastningsfullmakt*

(1) Denne bestemmelsen gjelder for

a) avtale mellom kontohaveren og institusjonen om fast betalingsoppdrag der belastning skal kunne skje etter krav fra betalingsmottakeren eller foretas av institusjonen av eget tiltak

b) avtale mellom kontohaveren og betalingsmottakeren om at kontoen gjentatte ganger skal kunne belastes etter krav fra betalingsmottakeren.

(2) Kontohaveren skal gi institusjonen skriftlig melding om avtale som nevnt i første ledd bokstav b.

(3) Institusjonen skal påse at de belastninger som foretas, ligger innenfor avtalens grenser.

(4) Avtalen skal på en entydig måte identifisere betalingsmottakeren. For hver betalingsmottaker skal avtalen angi en høyeste belastningsgrense og det tidsrommet belastningsgrensen knytter seg til.

(5) Dersom ikke annet er uttrykkelig avtalt, skal institusjonen sørge for at varsel sendes til kontohaveren senest sju virkedager før belastningen finner sted. Varslet skal opplyse om tidspunktet for når belastningen vil finne sted, om

Figur 3.7

betalingsmottakeren og om beløpets størrelse. Varslet kan tas med i kontoutskrift som nevnt i § 30 annet ledd annet punktum.

(6) Kontohaveren kan endre eller tilbakekalle fullmakten ved melding til institusjonen. Institusjonen skal gjennomføre endringen eller tilbakekallet senest første virkedag etter at meldingen er kommet fram.

§ 27. *Renteberegning ved godskriving og belastning av konto*

(1) Ved innskudd i kontanter skal renter av beløpet godskrives senest fra og med første kalenderdag etter at innskuddet ble foretatt. Ved annen godskriving av konto skal renter av beløpet godskrives fra og med oppgjørsdagen.

(2) Ved uttak i kontanter skal renter av beløpet godskrives til og med siste kalenderdag før uttaket. Ved uttak i kontanter på lørdag, helligdag eller offentlig høytidsdag skal renter av beløpet godskrives til og med siste kalenderdag før siste virkedag før uttaket. Ved annen belastning av konto skal renter av beløpet godskrives til og med kalenderdagen før oppgjørsdagen.

(3) Med oppgjørsdagen menes den kalenderdagen da godskriving eller belastning av kontoer kan inngå i oppgjøret mellom institusjonene og Norges Bank eller på annen måte gjøres opp institusjonene imellom. Ved overføring innen samme institusjon forstås med oppgjørsdag den dag godskriving og belastning av kontoene skjer.

(4) Kongen kan gi forskrift med regler om renteberegning på særlige områder og regler til utfylling og avgrensning av paragrafen her.

§ 28. *Tilbakekall og endring*

(1) Tilbakekaller eller endrer betaleren et betalingsoppdrag, skal den institusjonen som forestår betalingsoverføringen, medvirke til dette. For en bestemt type betalingsoppdrag kan det likevel avtales at betaleren ikke skal kunne kreve tilbakekall eller endring.

(2) Et betalingsoppdrag kan ikke tilbakekalles eller endres etter at betaling har skjedd, jf. § 39 første ledd.

(3) For tilbakekall av sjekker gjelder reglene i sjekkloven.

§ 29. *Tilbakeholdsrett og motregning*

(1) Institusjonen kan ikke utøve tilbakeholdsrett eller foreta motregning i innestående på konto, unntatt for forfalte krav som springer ut av kontoavtalen. Institusjonen kan likevel utøve tilbakeholdsrett eller foreta motregning for krav som er oppstått som følge av et straffbart forhold.

(2) Institusjonen kan ikke utøve tilbakeholdsrett eller foreta motregning i betalingsmidler som institusjonen har til disposisjon for å utføre betalingsoppdrag.

(3) Retting av feilaktige godskrivinger reguleres av § 31.

(4) Reglene i paragrafen her er ikke til hinder for at det etter ellers gjeldende regler stiftes særskilt sikkerhetsrett i innskudd.

Figur 3.8

IV. Føring av konto

§ 30. *Kontoinformasjon*

(1) Institusjonen skal jevnlig, og minst én gang i året, skriftlig informere kontohaveren om rente- og gebyrsatser for alternative typer innskuddskontoer som institusjonen tilbyr.

(2) Kontoutskrift skal sendes kontohaveren etter årets utgang. For lønnskonto, driftskonto og lignende brukskonto skal kontoutskrift sendes minst hver måned dersom det har vært bevegelse på kontoen.

(3) Hver kontoutskrift skal inneholde saldo, alle bevegelser på kontoen siden forrige utskrift, tidspunkter for renteberegninger for de enkelte bevegelser, gebyrer siden forrige utskrift og samlet fra siste årsskifte, påløpte renter og de rente- og gebyrsatser som gjelder for kontoforholdet. Navn på betalingsmottakere skal om mulig opplyses.

(4) Dersom kontohaveren har fått uriktige opplysninger om disponibelt beløp på kontoen og i god tro har belastet kontoen for større beløp enn disponibelt, kan institusjonen ikke kreve overtrekksrente av kontohaveren før kontohaveren har fått rimelig tid til å rette på forholdet.

§ 31. *Feilaktig godskriving av konto*

(1) Hvis institusjonen ved en feil har godskrevet uriktig konto eller uriktig beløp, kan institusjonen rette feilen ved å belaste kontoen innen utløpet av tredje virkedag deretter. Det samme gjelder dersom en institusjon ved en feil har godskrevet en konto i annen institusjon for så vidt den har adgang til å rette feilen i forhold til denne institusjonen.

(2) Institusjonens adgang til å rette feil etter første ledd gjelder ikke dersom godskriving av kontoen har skjedd i samsvar med oppdrag fra en tredjeperson.

(3) Hvis godskriving som nevnt i første ledd har sammenheng med straffbart forhold fra betalingsmottakerens side, eller fra en annen som har rett til å belaste betalingsmottakerens konto, kan institusjonen i alle tilfelle foreta retting av kontoen.

(4) At institusjonen ikke har adgang til å foreta retting av kontoen etter paragrafen her, er ikke til hinder for at institusjonen kan kreve tilbakesøking etter alminnelige regler.

§ 32. *Feilaktig belastning av konto*

(1) Hvis institusjonen ved en feil har belastet en konto, skal den uten ugrunnet opphold godskrive kontoen for et tilsvarende beløp.

(2) Institusjonen plikter uten hensyn til skyld å erstatte rentetap og annet direkte tap som er oppstått ved den feilaktige belastningen.

(3) For indirekte tap svarer institusjonen etter alminnelige erstatningsregler.

§ 33. *Melding om feil*

Oppdager institusjonen at en konto er feilaktig godskrevet eller belastet, skal kontohaveren underrettes uten ugrunnet opphold. Dersom feilen er rettet på en slik måte at det ikke er noen reell mulighet for at kontohaveren kan ha fått uriktige opplysninger om disponibelt beløp på kontoen, er det likevel tilstrekkelig at underretningen gis i forbindelse med en kontoutskrift.

Figur 3.9

V. Andres misbruk av konto og betalingsinstrument

§ 34. *Andres misbruk av konto m.v.*

(1) Kontohaveren er ikke ansvarlig for andres urettmessige uttak eller annen belastning med mindre den som har foretatt disposisjonen, har legitimert seg i samsvar med reglene i kontoavtalen, og belastningen har vært mulig som følge av forsett eller grov uaktsomhet fra kontohaveren eller fra noen som etter kontoavtalen har rett til å belaste kontoen.

(2) Ansvaret etter første ledd er begrenset til disponibelt beløp på kontoen på belastningstidspunktet. Er misbruk skjedd ved bruk av elektroniske betalingsinstrumenter innenlands, kan ansvaret heller ikke overskride belastningsgrenser som gjelder for den eller de bruksmåter som er benyttet. Begrensningene i leddet her gjelder ikke dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har medvirket forsettlig til at vedkommende kunne legitimere seg.

(3) Kontohaveren svarer ikke for andres urettmessige bruk som finner sted etter at institusjonen har fått varsel om forhold som skaper særlig fare for misbruk, som f.eks. at et betalingsinstrument er kommet bort eller at kode eller annen sikkerhetsprosedyre kan ha blitt tilgjengelig for uvedkommende. Kontohaveren er likevel ansvarlig dersom kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, forsettlig har muliggjort bruken.

(4) Uten hensyn til reglene i denne paragrafen er kontohaveren i alle tilfelle ansvarlig for tap som skyldes at kontohaveren eller noen som etter kontoavtalen har rett til å belaste kontoen, har utvist eller medvirket til svik mot institusjonen.

(5) Ansvaret ved misbruk av betalingskort er regulert i § 35.

§ 35. *Misbruk av betalingskort*

(1) Kontohaveren svarer med inntil kr 800 for tap som skyldes andres urettmessige bruk av betalingskort når tilhørende personlig kode eller annen lignende sikkerhetsprosedyre er brukt.

(2) Kontohaveren svarer med inntil kr 8.000 for tap som skyldes andres urettmessige bruk av betalingskort dersom

a) kontohaveren eller noen betalingskortet er overlatt til, ved grov uaktsomhet har muliggjort misbruket, eller

b) misbruket er muliggjort fordi kontohaveren eller noen betalingskortet er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til at betalingskortet er kommet bort eller innen rimelig tid etter at dette burde vært oppdaget.

(3) Er misbruk av elektronisk betalingskort skjedd innenlands, kan ansvaret etter annet ledd ikke overskride de belastningsgrenser som gjelder for den eller de bruksmåter som er benyttet.

(4) Begrensningene i annet og tredje ledd gjelder ikke dersom kontohaveren eller noen kortet er overlatt til, forsettlig har muliggjort bruken av kortet. Begrensningene gjelder heller ikke for tap som er oppstått som følge av at kontohaveren eller noen kortet er overlatt til, har unnlatt å underrette institusjonen snarest mulig etter å ha fått kjennskap til irregulær bruk av kortet.

(5) § 34 tredje og fjerde ledd gjelder tilsvarende for kontohaverens ansvar etter paragrafen her.

Figur 3.10

(6) Kongen kan i forskrift bestemme at reglene i paragrafen her skal gjelde helt eller delvis for andre typer betalingsinstrumenter.

§ 36. *Lemping av kontohaverens ansvar*

(1) Ansvaret etter §§ 34 og 35 kan lempes dersom måten kontoen kan disponeres på ikke er betryggende, eller dersom betalings- eller kontokortsystemet ikke oppfyller forsvarlige standarder for identifikasjons-, kontroll- og varslingsrutiner, og den urettmessige belastning eller misbruket har sammenheng med dette. Det kan også tas hensyn til manglende aktsomhet eller andre forhold på institusjonens side som har medvirket til at den urettmessige belastningen eller misbruket kunne skje.

(2) Kontohaverens ansvar kan også nedsettes dersom en leverandør av varer eller tjenester som har mottatt betalingen, forsto eller burde forstå at bruken av betalingsinstrumentet var urettmessig.

§ 37. *Reklamasjon. Tilbakeføring*

(1) I den utstrekning kontohaveren ut fra reglene i § 34 eller § 35 bestrider å ha ansvar for en belastning, skal institusjonen tilbakeføre beløpet og erstatte rentetap fra belastningstidspunktet, forutsatt at kontohaveren setter frem krav om tilbakeføring uten ugrunnet opphold etter at denne ble eller burde ha blitt kjent med forholdet. Plikten til tilbakeføring etter første punktum gjelder ikke for egenandel etter § 35 første ledd.

(2) Første ledd gjelder ikke dersom

a) kontohaveren skriftlig har erkjent ansvar for belastningen, eller

b) institusjonen innen fire uker fra mottakelse av skriftlig innsigelse fra kontohaveren har anlagt søksmål eller brakt saken inn for en nemnd som nevnt i § 4 første ledd.

(3) Blir saken avvist av en nemnd eller en domstol, løper en ny frist på fire uker, fra den dagen institusjonen ble kjent med avvisningen.

VI. Forholdet mellom betaler og mottaker ved betalingsoverføringer

§ 38. *Oppgjørsmåte*

(1) Betaling kan foretas ved overføring av beløpet til mottakerens konto med mindre annet er avtalt eller mottakeren har bedt om utbetaling med kontanter.

(2) Mottakeren kan gi nærmere anvisning om betalingsmåten, dersom dette ikke medfører vesentlig merutgift eller andre ulemper for betaleren.

(3) En forbruker har alltid rett til å foreta oppgjør med tvungne betalingsmidler hos betalingsmottakeren.

§ 39. *Tid og sted for betaling*

(1) Dersom betaleren har rett til å foreta oppgjør ved overføring til mottakerens konto, anses betalingen for å være skjedd når beløpet er godskrevet mottakerens institusjon. Ved overføring innen samme institusjon anses betaling for å være skjedd når beløpet er godskrevet mottakerens konto. Når oppgjør skal skje ved utbetaling i kontanter, anses betalingen for å ha skjedd når beløpet er stilt til mottakerens disposisjon gjennom bank på mottakerens sted og melding om dette er kommet frem til mottakeren.

Figur 3.11

(2) Dersom ikke annet er avtalt, anses dessuten en fastsatt betalingsfrist for å være avbrutt

a) ved betaling fra forbruker når betalerens oppdrag er mottatt av en finansinstitusjon

b) når mottakeren mottar og aksepterer sjekk eller annet betalingsmiddel.

(3) Dersom et mottatt betalingsoppdrag ikke skal utføres straks, regnes avbruddet av betalingsfristen fra den avtalte betalingsdagen.

(4) Betalingsfristen avbrytes ikke dersom betalingsoppdraget ikke blir gjennomført og dette skyldes betalerens eget forhold. Institusjonen skal i så fall varsle betaleren om dette uten ugrunnet opphold, med mindre annet er bestemt i eller i medhold av lov.

Figur 3.12

Norges offentlige utredninger 2007 og 2008

Statsministeren:

Arbeids- og inkluderingsdepartementet:
Om grunnlaget for inntektsoppgjørene 2007. NOU 2007: 3.
Ny uførestønad og ny alderspensjon til uføre. NOU 2007: 4.
Om grunnlaget for inntektsoppgjørene 2008. NOU 2008: 10.
Yrkessykdommer. NOU 2008: 11.
Skift og turnus – gradvis kompensasjon for ubekvem arbeidstid. NOU 2008: 17.

Barne- og likestillingsdepartementet:
Kvinner og homofile i trossamfunn. NOU 2008: 1.
Kjønn og lønn. NOU 2008: 6.
Med barnet i fokus. NOU 2008: 9.

Finansdepartementet:
Meglerprovisjon i forsikring. NOU 2007: 1.
En vurdering av særavgiftene. NOU 2007: 8.
Om tiltak mot hvitvasking og terrorfinansiering. NOU 2007: 10.
Individuell pensjonsordning. NOU 2007: 17.
Kulturmomsutvalget. NOU 2008: 7.
Revisjonsplikten for små foretak. NOU 2008: 12.
Eierkontroll i finansinstitusjoner. NOU 2008: 13.
Om foretaksstyring og tiltak mot manipulering av finansiell informasjon. NOU 2008: 16.
Skadeforsikringsselskapenes virksomhet. NOU 2008: 20.

Fiskeri- og kystdepartementet:
Retten til fiske i havet utenfor Finnmark. NOU 2008: 5.

Fornyings- og administrasjonsdepartementet:
Offentlig innkreving. NOU 2007: 12.

Forsvarsdepartementet:
Et styrket forsvar. NOU 2007: 15.

Helse- og omsorgsdepartementet:
Fordeling av inntekter mellom regionale helseforetak. NOU 2008: 2.

Justis- og politidepartementet:
Lovtiltak mot datakriminalitet. NOU 2007: 2.
Frarådningsplikt i kredittkjøp. NOU 2007: 5.
Fritz Moen og norsk strafferettspleie. NOU 2007: 7.
Rosenborgsaken. NOU 2007: 9.
Den nye sameretten. NOU 2007: 13.
Samisk naturbruk og rettssituasjon fra Hedmark til Troms. NOU 2007: 14.
Ny skiftelovgivning. NOU 2007: 16.
Fra ord til handling. NOU 2008: 4.
Bourbon Dolphins forlis den 12. april 2007. NOU 2008: 8.
Barn og straff. NOU 2008: 15.
Fiskefartøyet "Western"s forlis 6. februar 1981. NOU 2008: 19.
Nettbankbasert betalingsoverføring. NOU 2008: 21.

Kommunal- og regionaldepartementet:

Kultur- og kirkedepartementet:

Kunnskapsdepartementet:
Formål for framtida. NOU 2007: 6.
Studieforbund – læring for livet. NOU 2007: 11.
Sett under ett. NOU 2008: 3.
Fagopplæring for framtida. NOU 2008: 18.

Landbruks- og matdepartementet:

Miljøverndepartementet:

Nærings- og handelsdepartementet:

Olje- og energidepartementet:

Samferdselsdepartementet:

Utenriksdepartementet:
Samstemt for utvikling? NOU 2008: 14.

Offentlige publikasjoner

Opplysninger om abonnement,
løssalg og pris får man hos:
Akademika AS
Avdeling for offentlige publikasjoner
Postboks 84 Blindern, 0314 Oslo
E-post: offpubl@akademika.no
Telefon: 22 18 81 00
Faks: 22 18 81 01
Grønt nummer: 800 80 960

Publikasjonen er også tilgjengelig på
www.regjeringen.no