Universitetet
i Stavanger

Betalingsformidling i endringens tegn

En kvalitativ undersøkelse av endringer i verdikjeden for betalingsformidling og dets innvirkning på samfunnssikkerheten

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vår, semesteret 2019 Åpen
Forfatter: Andreas Schei Andersen	Andreas Schei Andersen signatur forfatter
Fagansvarlig: Bjørn Ivar Kruke Veiledere: Riana Steen UiS, Brynjel Johnsen Bits AS	
Tittel på masteroppgaven: Betalingsformidling i endringens tegn - En kvalitativ undersøkelse av endringer i verdikjeden for betalingsformidling og dets innvirkning på samfunnssikkerheten. Engelsk tittel: Payment transmission through the wind of changes - A qualitative study of changes in the value chain for payment services and its impact on societal security.	
Studiepoeng: 30 stp.	
Emneord: risiko, samfunnssikkerhet, endringstakt, kompleksitet, kaskadeeffekter, styring, kompetansebortfall, betalingsformidling, betalingstjenester	Sidetall: 99 + referanseliste og vedlegg: 120 Stavanger, 14.06.19

Forside for masteroppgave

Det teknisk-naturvitenskapelige fakultet

Forord

Denne oppgaven markerer slutten på mitt toårige studie ved Universitetet i Stavanger. Utarbeidelsen av oppgaven har vært en lang, lærerik og ytterst krevende prosess, hvor jeg sitter igjen med utrolig mye kunnskap. I prosessen har jeg fått uvurderlig hjelp fra en rekke mennesker. Først og fremst vil jeg takke Brynjel Johnsen ved Bits AS for sårt tiltrengt assistanse og sin dype innsikt i norsk betalingsformidling og veileder Riana Steen ved Universitetet i Stavanger for gode råd, strenge beskjeder og god veiledning i prosessen. Videre vil jeg takke alle informantene som tok seg tid til å stille opp og samtidig dele sin kunnskap. Jeg vil også takke min far for alle leksjoner, uvurderlige råd og rollen du har tatt på deg som min personlige rådgiver. Mor, søster og Mariell vil jeg også takke for korrekturlesing og hjelp med formuleringer.

Avslutningsvis vil jeg takke mine medstudenter og venner. En særegen takk til gutane, Sondre, Sondre og Anders. Takk for to år med hardt arbeid, tunge dager, glede, latter og lange lunsjer.

Andreas Schei Andersen.

Sammendrag

Den store endringstakten i finansnæringen generelt, og betalingsformidlingen spesielt har introdusert nye måter å gjennomføre betalinger, reguleringer og videre konsekvenser. Stor endringstakt er i natur forbundet med økt risiko og hendelser som innvirker på ens evne til å operere som normalt. En konsekvens av de store endringene i betalingsformidling er kan forventes å være inntog av nye aktører. Hensikten med studien er å avdekke hvorvidt nye aktører i betalingsformidlingen kan medføre konsekvenser for samfunnssikkerheten, av dette kan følgende problemstilling utledes:

Hvilke potensielle konsekvenser kan introduksjon av nye aktører i betalingsformidlingen ha for samfunnssikkerheten?

For å underbygge problemstillingen er det presentert tre forskningsspørsmål. Første forskningsspørsmål forsøker å avdekke gjennom hvilke nye kanaler nye aktører introduseres til norsk betalingsformidling. Det andre forskningsspørsmålet vurderer hvilke sårbarheter nye aktører kan skape i norsk betalingsformidling, herunder også hvordan de kan påvirke eksisterende sårbarheter. Siste og tredje forskningsspørsmål forsøker å avdekke de potensielle konsekvensene nye aktører kan ha for norsk betalingsformidling.

I besvarelsen av forskningsspørsmålene er det utelukkende benyttet empiri for å besvare de to førstnevnte, da deres utforming ikke ga videre grunnlag for en teoretisk vurdering av disse. Til å besvare sistnevnte forskningsspørsmål og overordnet problemstilling er det gjennomført en analyse bygget på *Normal Accidents* og organisatoriske ulykker for å illustrere om betalingssystemet endres som en følge av nye aktører. Videre er det benyttet et barriereperspektiv for å vurdere betalingsformidlingens sikring av sentrale funksjoner. Prinsippene for beredskap- og samfunnssikkerhetsarbeid benyttes for å vurdere hvordan foretakenes arbeid med beredskap og sikkerhet påvirkes av nye aktører. På bakgrunn av disse teoriene vurderes nye aktører til å ha en begrenset innvirkning på betalingsformidlingen og dets sikkerhet, herunder samfunnssikkerheten.

Abstract

The current changes affecting the finance sector and its closely related payment infrastructure have introduced new ways on how to initiate payments, new regulations and consequences. Fundamental changes are normally also attributed with enhanced risk which is due to affect the current system. One possible consequence of current changes in payments is the emergence of new actors. Regulations, new business platforms and strategic choices by current actors in Norwegian payments is believed to affect its current state. As such, this study will attempt to uncover how new actors may affect Norway's societal safety, which leads to the following thesis question:

Which potential consequences could the introduction of new actors in to payment initiation have for societal safety?

In order to adequately uncover the thesis question, three additional minor research questions have been included. The first question addresses how new actors are included in Norwegian payments. Furthermore, the second question revolves around what vulnerabilities new actors may create for the Norwegian payment infrastructure. Please note that the first two minor research questions are solely answered using empirical evidence, this is due to the wording of the questions and as such inclusion of theory would not provide additional analytical value. The third minor research question strives to uncover what possible consequences new actors included in the value chain for payments may have for the Norwegian sector for payments.

The study finds empirical evidence indicating inclusion of new actors may cause minor problems for the societal safety. The most prominent problem is due to outsourcing and its direct effect on the value chain for payments and possible loss of competence among the actors. PSD2 and the open banking platform is expected to include new actors in the system for payments, though only as payment initiation or providing account information for the customer. The interbank- and settlement system is not notably affected by the current expansion of players within payments, due to its strict regulation and limited access.

Innholdsfortegnelse

Liste over figurer og tabeller

Figurer

Tabeller

Liste over akronymer

Forkortelse	Betydning
BALTUS	BAnkenes on-Line TransaksjonsUtvekslingsSystem
BOLS	Bankenes On-Line Standard
BSK	Bankenes Standariseringskontor
CLS	Continuous Linked Settlement
DSB	Direktoratet for samfunnssikkerhet og beredskap
EBA	European Banking Authority
EDB	Elektronisk databehandling
EDIFACT	Electronic Data Exchange for Administration, Commerce and Transport
EFTPOS	Electronic funds transfer at point of sale
EKOM	Elektronisk kommunikasjon
FOI	Felles operasjonell infrastruktur
FNO	Finans Norge
KAR	Konto og adresseringsregister
IKT	Informasjon- og kommunikasjonsteknologi
NBO	Norges Banks Oppgjørssystem
NFC	Near field communication
NICS	Norwegian Interbank Clearing System
NIBE	Norsk interbank standard – EDIFACT
NNI	Nets Norge Infrastruktur
NOU	Norsk offentlig utredning
RTGS	Real-time gross settlement
P2P	Peer-to-peer
P2B	Peer-to-business
PSD2	Payment Services Directive 2
SWIFT	Society for Worldwide Interbank Financial Telecommunications
VPO	Verdipapiroppgjøret

Ordliste:

Barriere - Karakteristikken beskriver barrierer som en hindring som kan innvirke på hvorvidt en uønsket hendelse inntreffer og konsekvensene ved uønskede hendelser (Hollnagel, 2004, s. 68).

Bigtech – Betegnelse brukt om større teknologiselskap.

Fintech – Samlebegrep om ny finansiell teknologi og nye aktører som tilby finansielle tjenester.

Organisatoriske ulykker – ulykker med store konsekvenser knyttet til seg. Gjerne betegnet som systemulykker eller *Normal Accidents.*

Open banking - Forretningsstruktur hvor informasjon deles gjennom APIer til tredjepartsaktører (Brodsky & Oakes, 2017, s. 2).

Outsourcing - Overførsel av oppgaver/arbeid fra en organisasjon til en ekstern tilbyder (Power, Desouza & Bonifazi, 2006, s. 3).

Offshoring - Overførsel av oppgaver som støtter inn- og utlandsaktiviteter til utlandet, enten gjennom interne eller eksterne aktører (Larsen, Manning & Pedersen, 2013, s. 533).

Risiko - refererer til usikkerheten om og alvorligheten knyttet til hendelser og konsekvenser av en aktivitet med hensyn til hva mennesket verdsetter (Aven & Renn, 2010, s. 3).

Systemrisiko - En hendelse som grenser mellom naturlige hendelser, økonomisk, sosial og teknologisk utvikling, herunder også handlinger drevet av policy (Renn, 2008, s. 5).

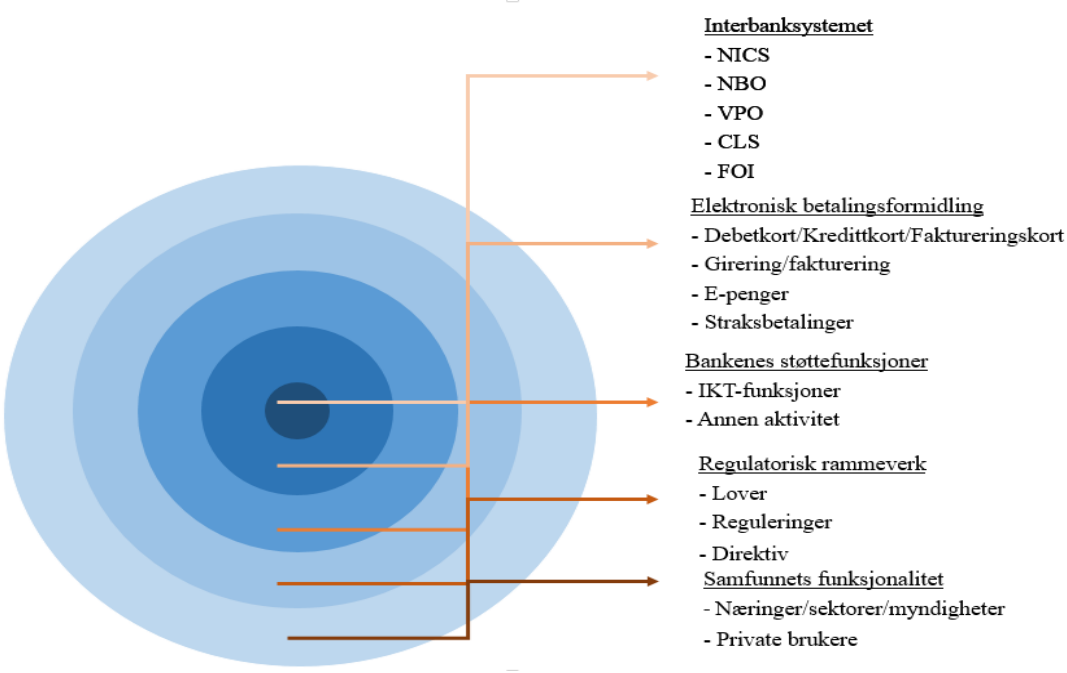
Sårbarhet - Et systems forutsetninger for eller manglende evne til å fungerer under og etter at det utsettes for en uønsket hendelse. Engen et al., 2016, s. 47

Verdikjede – Et firmas strategisk viktige aktiviteter som produseres, leveres, støttes og markedsføres for økonomisk vinning (Porter, 1985, s. 36).

1. Introduksjon

Teknologi og samfunn blir stadig tettere innvevd og kravene til teknologiske tjenesters tilgjengelighet øker og blir derfor mer kritisk (Engen et al., 2016, s. 138). Teknologiens utbredelse skaper stadig flere avhengigheter mellom ulike komponenter. Dette gjelder også infrastrukturen og de kritiske samfunnsfunksjonene, som grunnet digitalisering og globalisering er avhengig av lange og til dels uoversiktlige verdikjeder (NOU 2015:13, s. 15). Samtidig introduserer globalisering og digitalisering nye løsninger og tjenester som tjener befolkningen (ibid.).

Globalisering og digitalisering har medført økt integrering av bank- og finanstjenester i samfunnet, dette øker betydningen av tjenestene. Betalingsformidling er noe som i økende grad integreres inn i samfunnet og med både nye løsninger og tjenester. Løsninger som nettbank, mobilbank og Vipps er trekk ved dette. Der hvor vi før betalte bussbilletten kontant uten behov for digital støtte, må nå lange digitale verdikjeder fungere for å kjøpe en buss- eller togbillett ved bruk av Vipps.



Figur 1, betalingstjenester i samfunnsperspektiv

Direktoratet for Samfunnssikkerhet og beredskap understreker i sin rapport «Samfunnets kritiske funksjoner - Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?» samfunnets behov for sikre finansielle tjenester og den økende sårbarheten gitt den pågående digitale utviklingen. Evnen til å ha tilgang på både betalingsmidler og muligheten til å gjennomføre finansielle transaksjoner er derfor sentralt for samfunnets funksjonalitet.

Betalingstjenesters rolle i samfunnet bli mer kritisk, særlig med tanke på å gi den enkelte tilgang på primærvarer som mat, drivstoff og kritiske varer (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 85). Figur 1 illustrerer de samfunnsmessige faktorene som omkranser og innvirker på betalingstjenester.

Betalingsformidlingen ventes å undergå endringer som en følge av trender og anvendelse av ny teknologi. Her ventes det også endringer i aktørbilde som vil inkludere nye tjenestetilbydere. Samtidig er det blant bankene en økende tendens til å utkontraktere støttetjenester knyttet til drift og utvikling av virksomheten. Disse trendene kan derfor ventes å ha konsekvenser for betalingsformidlingen.

1.1 Oppgavens bakgrunn

Finansnæringen i Norge er blant de mest digitaliserte og fremoverlente i bruken av ny teknologi og digitale løsninger. En konsekvens av dette er at næringen er blitt veldig IKT-intensiv og avhengig av forhold som støtter oppunder deres aktiviteter (NOU 2015:13, s. 168). Bankene kan vanskelig håndtere alle aktivitetene som støtter oppunder deres hovedvirksomhet. Det er derfor en økende tendens blant bankene til å utkontraktere tjenester og oppgaver (Finanstilsynet, 2018, s. 7; 2019, s. 8). Disse trekkene ved næringen, sammen med EU-direktivet PSD2[1], presenterer en måte å vurdere hvordan banker og betalingstjenester vil bli påvirket av en vesentlig endringstakt. Store endringstakter er i natur preget av risiko (Finanstilsynet, 2018, s. 11). Betalingstjenester kan som en følge interne og eksterne krefter i løpet av få år oppleve å se veldig annerledes ut. Konteksten, rutinene, geografisk lokasjon og faktorer som tidligere har vært sentralt for å kunne initiere betalinger kan på sikt bli mindre relevant. En kan i ytterste konsekvens oppleve at den formen som i dag benyttes for betaling ikke en gang lenger brukes, betaling som aktivitet kan forsvinne.

Opphavet til studiens tematikk stammer tilbake til våren 2018, i forbindelse med utarbeidelse av et tverrfaglig prosjekt. I en idemyldringsfase ble mange ideer tatt opp og vurdert, en av disse omhandlet outsourcing[2] og offshoring[3] av IT-bedrifters støttefunksjoner. Tematikken bli ikke tatt opp og utviklet den gang, men den forsøkes det nå – med en vri. Studien forsøker å besvare hvilke konsekvenser store endringer generelt, og spesifikk hvordan endringer i aktørbildet for betalingsformidling kan innvirke på samfunnssikkerheten.

[1] Payment Service Directive 2.
[2] Finanstilsynet betegner dette som utkontraktering.
[3] Finanstilsynet betegner dette som utkontraktering til utlandet.

1.2 Problemstilling og tilhørende forskningsspørsmål

Norsk betalingsformidling har siden 1950-tallet i økende grad samlet seg rundt felles løsninger for interbank- og betalingstjenester. Dette har resultert i en ytterst effektiv og sikker betalingsformidling. Nåværende trender introduserer nye aktører som kan ta del i dette økosystemet for betalinger, og konsekvensene knyttet til nye aktører er dog noe uvisst. Dermed utledes følgende problemstilling:

Hvilke potensielle konsekvenser kan introduksjon av nye aktører i betalingsformidlingen ha for samfunnssikkerheten?

Det er også hensiktsmessig å videre definere problemstillingen for å belyse problematikken. Nøkkelbegrepene verdikjede og samfunnssikkerhet kan særlig være diffuse og ergo fremgå som en grobunn til misforståelse. Bankenes verdikjede for betalingsformidling defineres i kapittel 2.1.1, sårbarhet og samfunnssikkerhet defineres i kapittel 3.1. Problemstillingen underbygges av tre forskningsspørsmål.

FS1: Hvordan introduseres nye aktører til betalingsformidlingskjeden i Norge?

FS2: Hvilke sårbarheter tilfører nye aktører norsk betalingsformidling?

FS3: Hvilke konsekvenser kan et bredere spekter av aktører ha for betalingsformidlingen i Norge?

FS1 belyser hvordan nye aktører introduseres til norsk betalingsformidling, herunder gjennom hvilke kanaler nye aktører inkluderes i verdikjeden. FS2 forsøker å avdekke hvilke sårbarheter nye aktører kan tilføre til systemet for betalingsformidling. Dette vil inkludere å kartlegge eksisterende sårbarheter i systemet for betalingsformidling i Norge, inkludert barrierer og beredskap. FS3 belyser hvordan tematikk presentert i FS1 og 2 kan medføre konsekvenser for betalingsformidlingen. Her vurderes det hvorvidt en kan anse at nye aktører bringer med seg konsekvenser for betalingsformidlingen. Forskningsspørsmålene presenterer det empiriske og analytiske grunnlaget som gir muligheten for å vurdere problemstillingen. Som gjennom diskusjon og analyse forsøker å besvare om et bredere aktørbilde i betalingsformidling innvirker på samfunnssikkerheten.

1.3 Oppgavens avgrensing

Studien begrenses til elektronisk betalingsformidling og tilhørende aktører, både nye og tradisjonelle aktører i Norge. Dette er delvis grunnet tilgjengelighet men også den særegne posisjonen norske betalingstjenester har. Studien har fokus på elektroniske betalingstjenester da det er disse som undergår endringer i aktørlandskapet. Bruk av kontanter blir derfor ikke hovedfokus, men heller en komponent i helheten som definerer norske betalingssystem. Videre belyses ikke oppgjør for valutahandel ved CLS og verdipapirhandel ved VPO til tross for deres sentrale del i NBO. Denne avgrensningen er gjort da hovedfokuset ligger på betalingsformidling og dets innvirkning i samfunnssikkerheten.

Det teoretiske rammeverket har hovedfokuset på *Normal Accident Theory (1999)* og flere moment fra Reason (1997) verk *Managing the risks of organizational accidents.* Videre er prinsippene for samfunnssikkerhet- og beredskapsarbeid i Norge inkludert da arbeidet knyttet til dette blir påvirket av flere aktører. Det er også redegjort for barriereperspektivet og konseptet forsvar i dybden. Den mangfoldige og diverse anvendelsen av teori søker å dekke helheten og kompleksiteten knyttet til betalingsformidlingen. Teorien anvendes kun i forbindelse med analyse av forskningsspørsmål 3 og i påfølgende besvarelse av problemstillingen. Årsaken til dette er formuleringen av FS1 og 2 ikke direkte åpner for en teoretisk analyse av funnene.

Det empiriske grunnlaget i denne studien belager seg på både primær- og sekundærdata. Primærdata baseres på 5 intervju med aktører innen banknæringen, både fra myndighetene, banker og tredjepartstilbydere av tjenester. Sekundærdataen benyttet i studien er i stor grad, men ikke eksklusivt, hentet fra diverse myndigheter og organisasjoner i form av NOUer, ROS-analyser, rapporter og årsrapporter fra sentrale organisasjoner i norsk betalingsformidling. Omfanget av empiriske funn er grunnen til at oppgaven overskrider anbefalt lengde. Forskningsspørsmål 1 og 2 er utelukkende analysert og besvart ved bruk av empiri, noe som ansees som hensiktsmessig da forskningsspørsmålene ikke direkte inviterer til en teoretisk analyse.

1.4 Oppgavens oppbygning

Av tabell 1, gis det en kort summering av oppgavens oppbygning og hva en kan forvente av de ulike kapitlene.

Tabell 1, skjematisk fremvisning av oppgavens struktur.

Kapittel	Innhold
1. **Introduksjon**	Aktualisering og bakgrunn for valg av tema. Videre vil problemstilling og forskningsspørsmål presenteres, samt studiens avgrensinger.
2. **Bankenes infrastruktur og trender**	Introduksjon av sentrale historiske utviklingstrekk ved betalingsformidling i Norge siden 1950-tallet, interbanksystemet og system for betalingstjenester.
3. **Teoretisk bakteppe**	Presentasjon av relevant teori t i studien, fokus rettet mot NAT, organisatoriske ulykker, barrierer og ledende prinsipp for beredskapsarbeid.
4. **Metodisk fremgangsmåte**	Forskningsdesign-, og prosess, utvikling av intervjuguide, utvalg av informanter og arbeidet med analyse presenteres her. Overveielser rundt reliabilitet, validitet og etiske vurderinger samt oppgavens styrker og svakheter presenteres.
5. **Fremleggelse av innsamlet empiri**	Presentasjon av primær- og sekundærdata. Besvarelse av forskningsspørsmål 1 og 2. Inkludert analyse av funnene og vurderinger om nye aktørers inngang og innvirkning på norsk betalingsformidling.
6. **Analyse/drøfting**	Analyse og drøfting av forskningsspørsmål 3 med bakgrunn i innsamlet empiri og teoribidrag. Avslutningsvis analyse og drøfting av studiens problemstilling.
7. **Konkluderende bemerkninger og veien videre**	Konklusjon basert på analyse og drøfting i kapittel 5 og 6. Videre drøftes mulige problemstillinger en videre kan se på for å belyse temaet videre.
8. **Referanseliste**	Presentasjon av kildene benyttet i studien.

2. Bankenes infrastruktur og verdikjede

Kapittelet presenterer grunntrekkene ved betalingsformidling i Norge. Først gis det en innføring i de største endringene og utviklingen av betalingstjenester og interbanksystemet i Norge de siste 50 årene. Videre vies det plass til en beskrivelse av nåværende trender innen næringen. Avslutningsvis presenteres bankenes verdikjede for betalingsformidling og kjerneoppgaver, dernest infrastrukturen for betalinger og transaksjoner i banksektoren.

2.1 Historisk tidslinje og trender for betalingsformidling

Først redegjøres det for de løsningene kundene møter. Så presenteres utviklingen innen infrastrukturen for betalingsinfrastrukturen. Presentasjonen er en del av forstudiet av historisk utvikling av betalingsformidling som er sentralt for studien, som kan leses i sin helhet i vedlegg 6. Skisseringen er ikke uttømmende og burde ikke ansees som en historisk gjengivelse, men gir en god oversikt over utviklingen.

2.1.1 Betalingsformidling i et historisk perspektiv

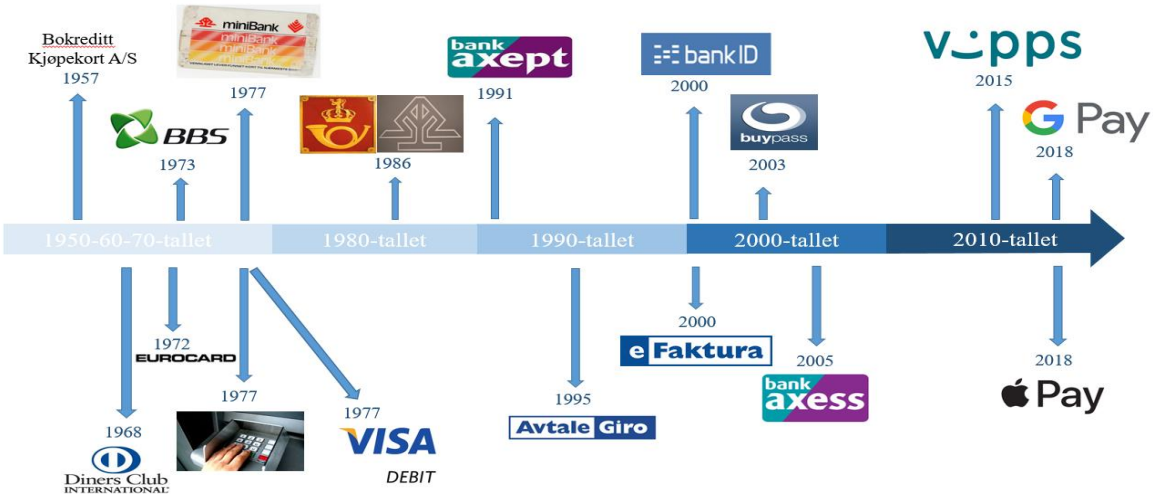
Tradisjonelt sett har bankvirksomhet handlet om forvaltning av et balanseprodukt. Kjerneaktivitetene innskudd og utlån har siden introduksjonen av den moderne banken i Italia i middelalderen (Ferguson, 2008, s. 48) blitt supplert med aktiviteter, deriblant betalingsformidling. I lang tid har tilgjengeliggjøring av betalingsmidler vært et sentralt virke for banker. Betalingsformidlingen i Norge i dag er blant de mest digitaliserte i verden. Kortbruken er høy sammenliknet med andre land, og bruk av kontanter tilsvarende lav (NOU 2015:13, s.168; Haare & Solheim, 2011, s. 26; Norges Bank, 2018b, s. 70). Et sentralt aspekt ved norsk betalingsformidling er at den i stor grad belager seg på selvregulering gjennom Finans Norge (NOU 2015:13, s. 170).

Tilgjengeliggjøring av elektroniske betalingstjenester

Utviklingen av elektroniske betalingstjenester i Norge kan betegnes som en stegvis prosess initiert av bankene og datasentralene. Opprettelse av datasentraler var viktig for bankene for å levere moderne og funksjonelle løsninger for EDB[4] og for kundene. De første betalingsløsningene knyttet til kort ble dog ikke introdusert av bankene. Kjøpekort utsted av møbelforhandlere og internasjonale kortselskap var de første til å tilby kortbetalinger. Bankene introduserte kort for bruk utenlands gjennom selskapet VISA AS i 1977 (Haare & Solheim, 2011, s. 55-57). 1984 var året nasjonale kort først ble introdusert. Kortene var derimot ikke kompatible med andre terminaler og minibanker enn de utstedt av kortutsteder

[4] Elektronisk databehandling

(ibid., s. 17). For å finne en felles løsning, gikk de ulike bankforeninger inn i bilaterale samarbeid. Dette kulminerte i 1991 til samordningen av alle EFTPOS[5]-system under BankAxept. Løsningen ble satt i drift 1993 og er blitt en sentral FOI[6] i norsk betalingsformidling. I 2005 ble tjenesten BankAxess også innlemmet her (ibid., s. 29). Gireringstjenester har utviklet seg på lignende måte som kortbetalinger, men samordningen mellom bankforeningene og postverket tok lengre tid. Først på 1990-tallet var det tegn til progresjon i samordningsprosessen. Dette resulterte i innføringen av en felles giroblankett i 1996. Løsningene AutoGiro og AvtaleGiro ble også introdusert som følge av samordningen (Haare & Solheim, 2011, s. 128). Parallelt med ferdigstillingen knyttet til samordning av kort- og girotjenester på 1990-tallet introduserte digitaliseringstrenden nye muligheter for betalingsformidling og –tjenester. I Norge ble dette først tydelig da fire e-pengeforetak, inkludert BuyPass, fikk konsesjon i 2003 (Norges Bank, 2004, s. 31). Bankene begynte på slutten av 1990-tallet å tilby tradisjonelle banktjenester på internett, da via nettbank som ble introdusert i 1996 (Haare & Solheim, 2011, s. 139). Noen av tjenestene som ble introdusert til nettbanken var regningsbetalingstjenesten eFaktura og autentiseringstjenesten BankID (ibid., s. 30 & 208). Fremveksten av mobiltelefonen har også bidratt til nye tjenester. Allerede i 1994 ble Telegiro og Telebank introdusert (ibid., s. 139). Smarttelefonen har senere vært sentralt i introduksjonen av tjenester som Vipps, mCash og i senere år Google Pay og Apple Pay. Figur 2 under illustrerer deler av utviklingen av betalingstjenester.



Figur 2, tidslinje for sentrale endringer for betalingstjenester

[5] Electronic funds transfer at point of sale.
[6] Felles operativ infrastruktur.

Utvikling av interbanksystemet

Norges Bank har fungert som oppgjørsbank i Norge siden 1898 (Haare & Solheim, 2011, s. 34). Endringene i interbanksystemet har vært betydelige, med de største endringene etter 1960-tallet (Haare, 2007, s. 153). Økende digitalisering av systemer og fremveksten av datasentraler var drivkrefter i interbanksystemet frem til 1980-årene. Datasentralene var viktige i samordningsprosessen i interbanksystemet og standarder som kontonummer og KID-nummerering (Haare & Solheim, 2011, s. 63-64, 69). Fra midten av 1980-årene og utover begynte arbeidet med samordning av de ulike datasentralene for å operasjonalisere en felles samordning av interbanksystemet. Dette kulminerte i opprettelsen av avregningssystemet NICS[7] på 1990-tallet. NICS, sammen med Norges Bank Oppgjørssystem kjent som NBO, ga bankene et RTGS[8]-system med vesentlig lavere oppgjørsrisiko enn tidligere (ibid., s. 150).

Tabell 2, oversikt over utvikling av interbanksystemet

Funksjon	**Tid for introduksjon**
Kontonummer	Innført i 1967
KID-nummerering	Innført i 1973
Bankenes On-Line Standard	Innført på 1970-tallet
Medlemskap i SWIFT[9]	Siden 1974
Norsk InterBank-EDIFACT[10]	Innført 2000
BAnkenes on-Line TransaksjonsUtvekslingsSystem	Tatt i bruk i 1986
Norwegian Interbank Clearing System	I bruk siden 1993
Norges Bank Oppgjørssystem, RTGS-utgaven	I bruk siden 1999

Tabell 2 illustrerer standardene og systemer er introdusert i norsk betalingsformidling. Listen er ikke uttømmende, men illustrerer en prosess preget av samordning og internasjonale impulser. Tabellen viser hvordan betalingsformidlingen utviklet seg til å bli mer digitalisert gjennom EDB-teknologi. Felles operativ infrastruktur er ikke inkludert her. Stadfestelse av

[7] Norwegian Interbank Clearing System.
[8] Real-time gross settlement.
[9] Society for Worldwide Interbank Financial Telecommunications.
[10] Electronic Data Exchange for Administration, Commerce and Transport.

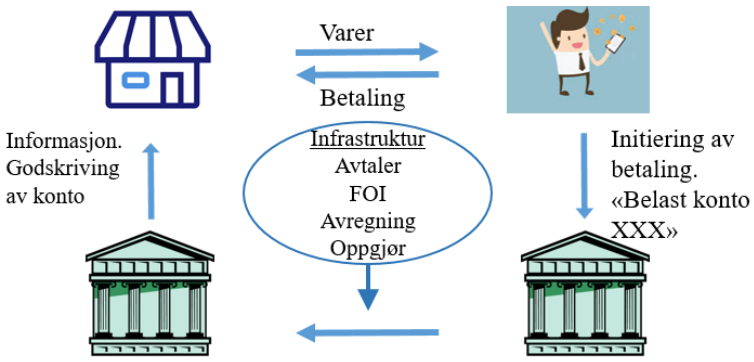
regler tilknyttet dette gjøres i dag av finansnæringens interesseorganisasjon, Finans Norge. Finans Norge er sentral for bankenes selvregulering (NOU 2015:13, s. 169-170).

2.2 Bankenes verdikjede og infrastruktur

Betalingssystemet i seg selv kan deles i to deler: systemet for betalingstjenester og interbanksystemet. Førstnevnte inkluderer bankenes verdikjede for betaling, dette ansees som *frontend*[11], altså bankenes utforming av løsningene som kundene bruker. Sistnevnte dreier seg om interbanksystemets infrastruktur som håndterer transaksjoner banker imellom, også betegnet som *backend*[12]-systemet. Herunder inkluderes FOIene, meldingsstandarder, lover, regler og reguleringer. (Finanstilsynet, 2018, s. 10; NOU 2015:13, s. 168; Solheim & Strømme, 2003, s. 206).

2.2.1 Bankenes verdikjede for betalingsformidling

Opphavet til den moderne banken fra Italia bygger på balanseproduktet som grunnlaget for bankvirksomhet (Ferguson, 2008, s. 44). Balanseproduktet har tradisjonelt omhandlet innskudd og utlån. Senere har derimot bankenes portefølje økt med blant annet aksjer, valuta, eiendom, forsikring og betalingsformidling. En konsekvens av dette er at bankene nå yter flere tjenester som er av viktighet for samfunnet (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 85), deriblant betalingsformidling. Figur 3 er en forenklet illustrasjon av gangen ved betalinger.



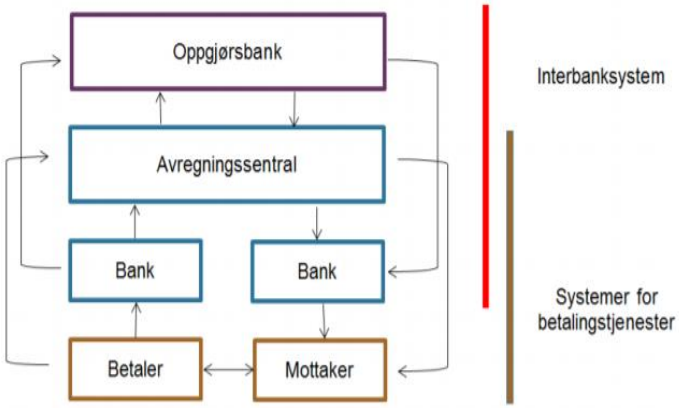
Figur 3, firkantmodellen for betalinger

Verdikjede er et uttrykk introdusert av Porter (1985), og uttrykket refererer til et firmas strategisk viktige aktiviteter som produseres, leveres, støttes og markedsføres for økonomisk vinning (Porter, 1985, s. 36). For å underbygge de produktive aktivitetene er banknæringen særs avhengig av IKT (NOU 2015:13, s. 180). Betalingstjenester i dag baseres på tekniske og digitale løsninger som mobil- og nettbank, noe som krever tilfredsstillende IKT-løsninger for sine brukere, noe som gjør IKT sentralt i norsk betalingsformidling (Norges Bank, 2018a, s. 2).

[11] Utformingen av løsningen som kunden møter
[12] Systemet som ligger bak løsningen som introduseres til brukeren

Betalingstjenester

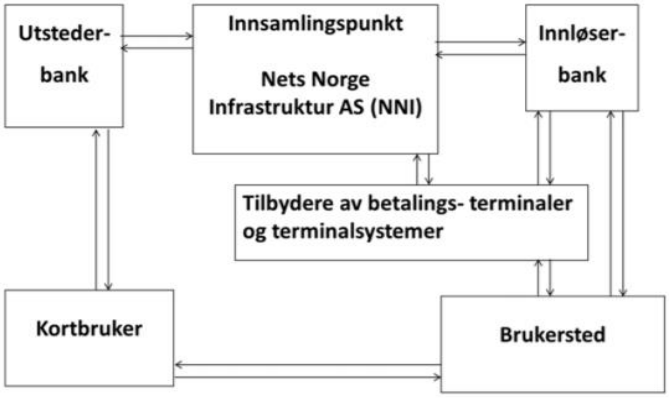
Systemet for transaksjoner involverer en rekke deltakere. Figur 4 illustrerer gangen ved betalinger og deltakende parter. Skillet mellom systemer for betalingstjenester overlapper med interbanksystemet. Figur 4 skiller derimot ikke imellom de ulike betalingstjenestene i norske betalingsmarkedet. Transaksjonene vil derimot uavhengig betalingstjeneste gå innom leddende illustrert av figuren. Sentralt for norsk betalingsformidling er samordning, derfor har betalingstjenestene i dag mange fellestrekk (NOU 2015:13, s. 168).



Figur 4, illustrasjon av transaksjonsflyt i betalinger av Norges Bank (2016a, s. 87)

Kortbetalinger

Det foreligger hovedsakelig tre betalingskort: debet-, kreditt- og faktureringskort. Kortbruken i Norge er tiltakende og BankAxept-løsningen er mest utbredt (Norges Bank, 2018b, s. 71). Løsningen benyttes til debetkorttransaksjoner, altså transaksjoner hvor transaksjonsbeløpet trekkes fra brukerens bankkonto (ibid., s. 70). For at butikker kan tilby betaling til BankAxept-kort, må de ha avtale med en bank som garantist for oppgjør av transaksjonene. Brukerne har en avtale med sin bank om at BankAxept-kortet er knyttet til sin konto. Idet kunden bruker kortet registreres kortinformasjonen ved terminalen, og kunden blir bedt om å verifisere transaksjonen ved pinkode. Dette sendes videre til et innsamlingspunkt hvor både pinkode og terminal autoriseres. Her gjennomføres dekningskontroll av kortet, noe som gjøres av utstederbank. Transaksjonsinformasjonen samles inn av NETS Norge Infrastruktur AS[13] og sendes til NICS for avregning (ibid., s. 71). De fleste BankAxept-kort er også utstyrt med betalingsløsningen til VISA. Dette er typisk en løsning som benyttes i utlandet, men også innenlands dersom transaksjonen ved kortterminaler ikke fungerer med BankAxept. Transaksjonsbeløpet til kortinnehaver er så reservert på konto, slik at det ikke kan brukes før avregning i NICS. BankAxept er et



Figur 5, transaksjonsflyt i BankAxept, av Norges Bank (2016a, s. 91)

[13] Også kjent under NNI

EFTPOS-system og en sentral del av den felles operative infrastrukturen i bankenes betalingsformidling (NOU 2015:13, s. 175).

Det er nå blitt mulig å gjennomføre EFTPOS-transaksjoner gjennom mobiltelefon, bank- eller kredittkort som er utstyrt med EMV[14]-teknologi og NFC[15]-løsninger. Bruken av mobiltelefon og kontaktløs betaling ved bruk av NFC-teknologi er økende (Norges Bank, 2018b, s. 72). Aktører som Apple, Garmin, Google og andre store TECH-selskaper tilbyr løsninger som baserer seg på tokenisering av betalingskort, som gjør det mulig å benytte smarttelefon eller –klokke for kontaktløs betaling ved terminaler.

Kredittkort debiterer ikke en konto disponert av brukeren, men det ytes i stedet kreditt til kortinnehaver (Norges Bank, 2018b, s. 70). Slike kort skiller seg fra de to andre korttypene ved at det ytes kreditt som kan betales tilbake i hele eller delvise transaksjoner eller ingenting. Uten nedbetaling vil det løpe renter på den utstedte kreditten. Kredittkort har også en maksgrense for hvor mye kreditt som ytes til kortinnehaver (ibid.). Kreditten som ytes til kortinnehaverne gis fra ulike foretak i samarbeid med betalingstilbyderne. Typiske tilbydere av slike betalinger er VISA eller MasterCard. Betalingstilbyderne sørger for at transaksjonen kommer til mottaker gjennom egne internasjonale clearingsystem. Faktureringskort er, som kredittkort ikke knyttet til en konto. For slike kort faktureres derimot kortinnehaver for bruken etter en endt periode (Norges Bank, 2018b, s. 70).

Nettbank og mobilbetalinger

Betaling av regninger og fordringer har siden 1950 gjennomgått store endringer; fra ulike papirbaserte girotyper blant bankene til samordning og nettbaserte løsninger som mobil- og nettbank (Haare & Solheim, 2011, s. 128; Norges Bank, 2018b, s. 75). Regninger er i dag tilgjengelige i enten mobil- eller nettbank gjerne gjennom betalingskravene eFaktura eller AvtaleGiro (Norges Bank, 2018b, s. 75). Konseptet om automatisert betaling AvtaleGiro er bygget på er eldre enn selve produktet, og gikk da under navnet Autogiro (Haare & Solheim, 2011, s. 137). Autogiro ble avløst av AvtaleGiro for personkunder, og gjelder nå kun for bedrifter (Bits AS, ingen dato(a)). AvtaleGiro gjelder da direkte debiteringer på en bedrifts utestående fordringer hos kundene ved en forfallsdato. Løsningen bygger på en avtale mellom banken og betaler om at banken kan overføre midler til en bedrift. Bedriften med fordringen

[14] Teknisk standard for betalinger.
[15] Near field communication.

angis i avtalene mellom betaler og bank (Bits AS, ingen dato(b)). Disse løsningene har tatt over for tele- og brevgiro som stadig minsker i omfang (Norges Bank, 2018c, s. 5).

Teknologi og globalisering er to faktorer som redefinerer arbeidsoppgaver og lønnsomhetspotensialet hos bedrifter og sektorer (Andersen & Sannes, 2018, s. 203). Inntoget av smarttelefoner presenterer en rekke muligheter for nye betalingstjenester og –løsninger (Haare & Solheim, 2011, s. 209). Utover å tilby tradisjonelle banktjenester på ny plattform, har mobil- og smarttelefonen åpnet for mobilbetalinger. Mobilbetalinger viser til betalinger som gjennomføres via en applikasjon på smarttelefon. Ved slike betalinger er applikasjonen ofte knyttet til et betalingskort som et underliggende betalingsinstrument, men transaksjonen kan også gjennomføres ved girobetaling (Norges Bank, 2018c, s. 6).

I tillegg til debitering, fakturering og kreditt finnes det ytterligere en form for betalingstjenester: e-penger. E-penger er digitale verdienheter og kan utelukkende benyttes for elektroniske betalinger, enten det er forhåndsbetalte betalingskort eller innestående verdier på en e-pengekonto (Norges Bank, 2016b, s. 88). E-pengeforetakene som tilbyr disse tjenestene må ha konsesjon fra norske myndigheter. Eksempler på slike betalingsforetak er PayPal og Revolut. PayPal er ikke en deltaker i det tradisjonelle norske interbanksystemet, ergo følger ikke e-pengeforetaket mønsteret i det norske betalingssystemet (Langbraaten, 2012, s. 17).

Fintechs og bigtechs er nye aktører som utvikler løsninger som kan konkurrere og samarbeide med det eksisterende tilbudet av betalingstjenester. De nye aktørene utvikler gode brukergrensesnitt som er attraktive for brukerne. Aktørene kan gjennom PSD2 eller bilaterale open-banking samarbeid tilby sine tjenester. Eksempelvis kan en se til fintechaktøren Payr, som har introdusert en nettbankløsning som forenkler brukerens oversikt over personlig økonomi (Payr, ingen dato). Videre vil applikasjonen råde brukerne til betalingsløsninger som er de mest gunstige for brukeren selv, i henhold til hva som er rimeligst, dette gjelder både strømleverandører, lån, forsikring og mobiltelefoni (Bakken, 2018). KLARNA er et eksempel på en annen Fintech-aktør som tilbyr betalingstjenester, særlig i forbindelse med netthandel.

2.2.2 Infrastruktur for betalingsformidling

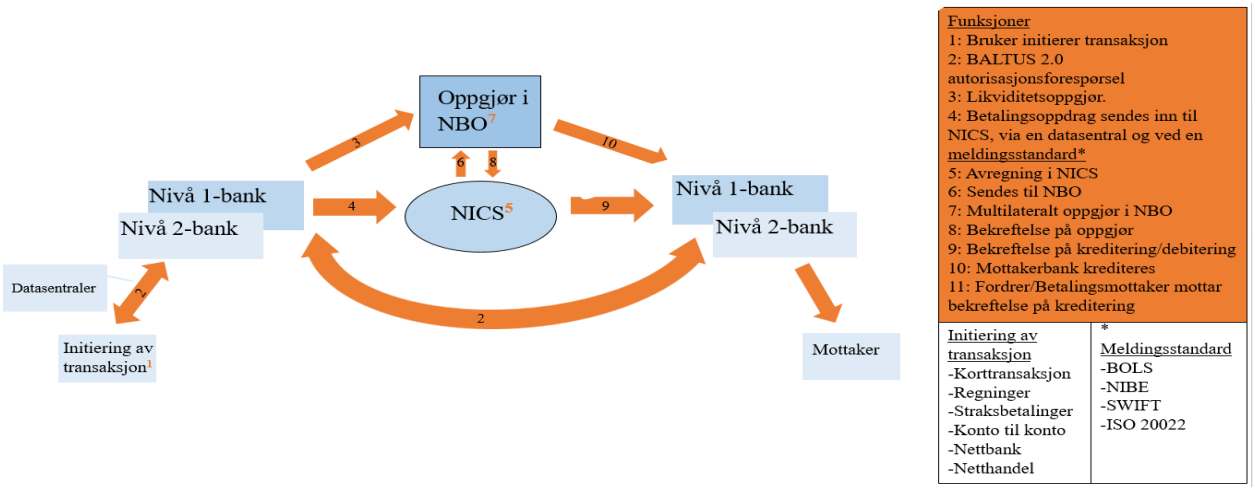
Finansiell infrastruktur består av flere systemer som gjør det mulig å gjennomføre transaksjoner. Samordningsprosessene i betalingsinfrastrukturen og betalingsformidlingen har medført at samfunnsmessige kostnader knyttet til betalingsformidling er det lavest i Europa. Ifølge Norges Bank (2014, s. 7) utgjør kostnadene 0,49% av BNP.

Interbanksystemet

Interbanksystemer er et system hvor banker overfører kapital seg imellom, og her foreligger det felles regler for avregning og oppgjør (Norges Bank, 2018a, s. 20). Sentralt i interbanksystemet ligger NBO og NICS. NICS er bankenes felles avregningssentral i henhold til definisjonen presentert i Betalingssystemloven (1999) § 1-1 første og andre ledd

> Med betalingssystem menes systemer for overføring av midler med formelle og standardiserte ordninger og felles regler for behandling, avregning eller oppgjør av betalingstransaksjoner. I et betalingssystem inngår interbanksystem eller systemer for betalingstjenester.
>
> Som interbanksystem regnes systemer basert på felles regler for avregning, oppgjør eller overføring av penger mellom kredittinstitusjoner. (Betalingssystemloven, 1999, § 1-1)

På bakgrunn av transaksjoner gjort av brukerne avregnes det i NICS hvor mye bankene skylder og har til gode hos hverandre. Avregningen sendes så til NBO for oppgjør, innsending og oppgjør skjer fem ganger om dagen. Bankenes saldo i Norges Bank justeres da i henhold til avregningene gjort i NICS (Norges Bank, 2018b, s. 68). Alle betalinger i norske kroner, både avregnings- og enkeltvisbetalinger gjøres opp i NBO (Norges Bank, 2018a, s. 24; Norges Bank, 2018b, s. 75). Alle bankene i Norge har konti i NBO, men det er kun de største bankene som gjør opp sine transaksjoner direkte i NBO. Mindre banker benytter seg av de større bankene som oppgjørsbanker. Dette betyr at de gjør sine avregningsoppgjør i oppgjørsbankene (Norges Bank, 2018b, s. 75).



Figur 6, Transaksjonsflyten i norske betalingssystemer (NOU 2015:13, s. 169) .

Figur 6 viser gangen i betalinger i det norske interbanksystemet. For betalinger innenlands benyttes NICS og er derfor en sentral del av det norske betalingssystemet. NBO er kjernen i alle oppgjør som har med norske konti å gjøre. Figuren skiller mellom nivå 1 og 2 banker.

Nivå 1 banker har direkte oppgjør i NBO, altså de større bankene som DNB, Sparebank 1 SMN og Danske Bank (Norges Bank, 2018a, s. 29). Bankene blir altså oppgjørsbank for nivå 2 banker, ergo at nivå 1 bankene tar nivå 2-bankenes stilling og deres posisjon i NBO (ibid.).

Felles operativ infrastruktur

Det finnes flere fellesløsninger som bankene benytter, disse utgjør den felles operative infrastrukturen, FOI. BankAxept er samordningen av kortløsninger blant kortutstedere og banker i Norge. Dette er det en av de mest sentrale FOIene, og løsningen er på alle debetbankkort. Ved bruk av et slikt kort trekkes beløpet fra brukerens konto gjennom transaksjonsløypen redegjort for i kapittel 2.2.1 (Norges Bank, 2018b, s. 70).

BankID er en elektronisk ID som også er den mest utbredte i Norge med over tre millioner brukere. Det er en sikkerhetsløsning for autentisering av personer ved bruk av elektroniske tjenester (NOU 2015:13, s. 170). BALTUS[16] 2.0 er knyttet opp til det norske betalingssystemet som en felles infrastruktur for informasjonsutveksling. Målet med tjenesten er å kunne enkelt formidle informasjon med økonomisk informasjon mellom ulike finansinstitusjoner (Bits AS, ingen dato(d)). Tjenesten er tett knyttet opp mot autorisering i BankAxept-løsningene, og omhandler informasjonsdistribuering knyttet til: betalinger med kort, minibanktransaksjoner, betalinger online gjennom BankAxess, straksbetalinger, sperring av debetkort knyttet til BankAxept, samt kontooverførsler (Bits AS, ingen dato(d)). Konto og adresseringsregister, også kjent som KAR, inneholder bankenes kontonummer og tilhørende kunde-id, samt mobilnummer for bruk av Straksbetalinger. KAR benyttes for å verifisere at betalingskontoer er gyldige og aktive, samt å avdekke kontoinnehaver (Bits AS, ingen dato(g)). Registeret bidrar til en mer effektivt og fleksibel bruk av kommunikasjon.

Standarder

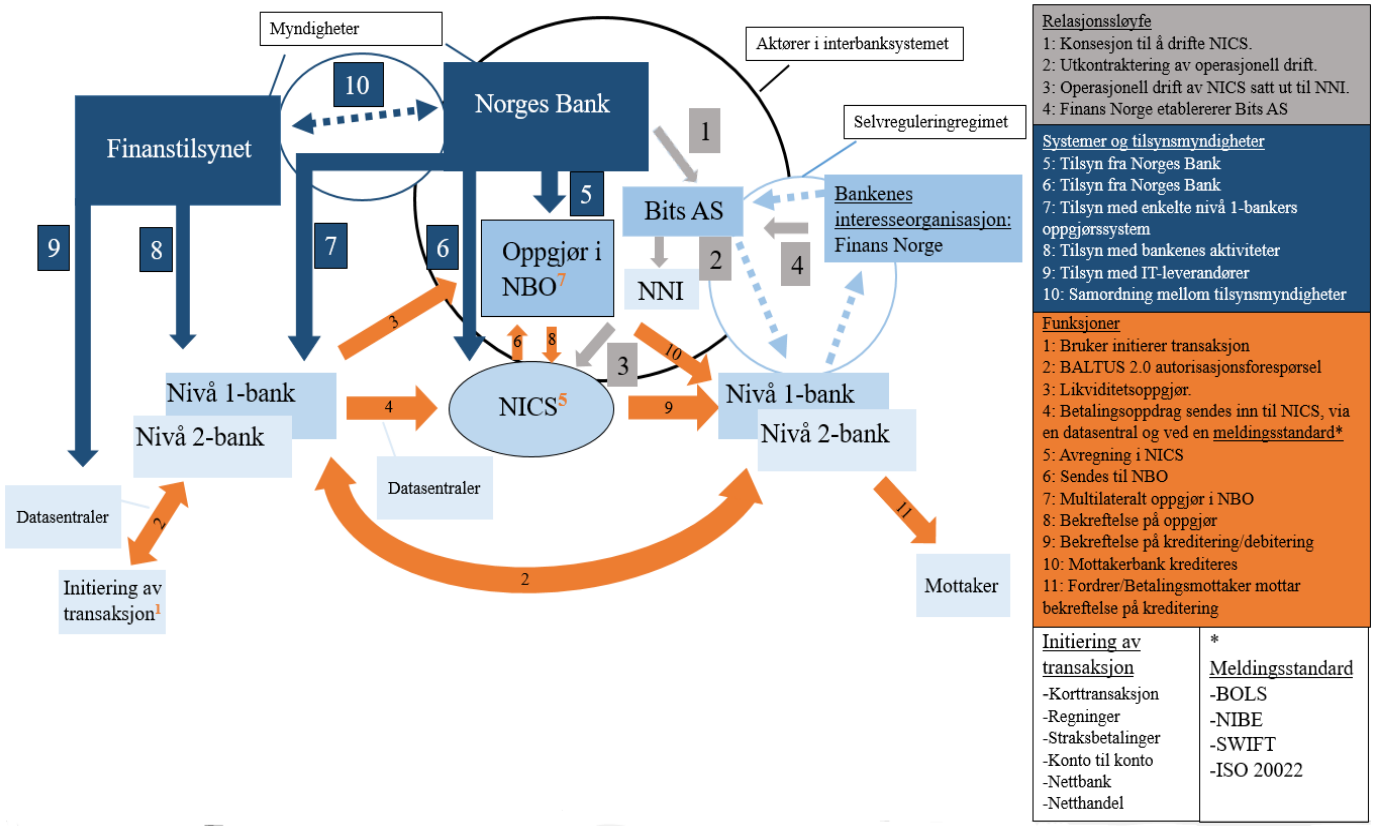
BOLS, Bankenes On-Line Standard, er et format som bankene bruker for informasjonsutveksling i NICS (Bits AS, ingen dato(e)). Standarden er lukket og er blitt brukt i det norske interbanksystemet siden slutten av 1970-tallet. Meldingsstandarden har tidligere vært brukt til kommunikasjon i interbanksystemet (Haare & Solheim, 2011, s. 165), men er i dag forbehold tre hovedmål: kapitaltransaksjon knyttet til transaksjoner; dekningskontroll; og utveksling av informasjon til bankene (Bits AS, ingen dato(e)). EDIFACT er en internasjonal meldingsstandard for forretningsdokumenter, standarden ble først tatt i bruk på 1990-tallet av norske banker. Det ble utviklet en norsk versjon av EDIFACT, Norsk InterBank-EDIFACT

[16] BAnkenes on-Line TransaksjonsUtvekslingsSystem

også kjent som NIBE. NIBE er en norsk standard for informasjonsutveksling mellom banker som er med i NICS (Bits AS, ingen dato(c)). ISO 20022 er en ny meldingsstandard som skal erstatte de lukkede nasjonale standardene for finansielle meldinger med filer som brukes i Norge (Bits AS, ingen dato(f)). Standarden dekker hele verdikjeden fra betaler til fordrer, fordelen ved bruk av en slik standard er dens anvendelighet. ISO 20022 kan anvendes til alle typer meldinger, den kan også brukes ovenfor banker utenlands. Arbeidet med innfasingen av denne meldingsstandarden er allerede påbegynt i Norge (ibid.).

Oppsummering kapittel 2

Av figur 7 kan en se hvordan utvikling, standarder, samordning, samspillet mellom myndigheter og bankere og deres interesseorganisasjon utgjør systemet for betalingsformidling i dag.



Figur 7, system for betalingsformidling

3. Teorigrunnlag

Kapittelet begynner med en redegjørelse av sentrale begreper innen samfunnssikkerhet. Videre presenteres Perrow (1999) og hans *Normal Accidents Theory*, som gir grunnlag for en vurdering av systemet for betalingsformidling. Dernest introduseres Reason (1997) og hans tanker rundt latente forhold og aktive feil, samt ulike mekanismer som kan medføre dette. Siden belyses ulike perspektiver på barrierer og tilhørende egenskaper ved dem. Avslutningsvis presenteres prinsippene for samfunnssikkerhet- og beredskapsarbeid.

3.1 Begrepsavklaring

En avklaring av sentrale begreper innenfor samfunnssikkerhet er hensiktsmessig, da en rekke av disse begrepene kan oppfattes som diffuse og ha flere meninger og bruksområder Videre finnes det lignende begreper i banknæringen med ulik betydning fra de lignende begrep innen samfunnssikkerhet, det blir derfor hensiktsmessig med en presisering.

3.1.1 Samfunnssikkerhet og samfunnets funksjonalitet

Samfunnssikkerhet er et omfattende begrep som kan defineres på ulike måter – alt etter som hvilke faktorer som vektlegges. Denne studien baseres på definisjonen presentert i Stortingsmelding 10. 2016-2017:

> Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger
>
> (Justis- og beredskapsdepartementet, 2016, s. 9).

Definisjonen fremhever en evne som samfunnet har til å beskytte og samtidig håndtere hendelser for å kunne tjene funksjoner og ivareta menneskers helse og liv. Samfunnets funksjonalitet og kritiske samfunnsfunksjoner er sentrale begrep som må redegjøres, for å vurdere viktigheten av betalingsformidling i det norske samfunn.

Samfunnets funksjonalitet, ansees som funksjoner og kapabiliteter som tjener befolkningen direkte for at samfunnet skal kunne fungere (Engen et al., 2016, s. 46). Direktoratet for samfunnssikkerhet og beredskap (2016) har identifisert syv hovedområder som er sentralt for samfunnet, herunder samfunnets funksjonalitet. Disse er forsyningssikkerhet; vann og avløp, finansielle tjenester, elektronisk kommunikasjon også kjent som EKOM; transport; satellittbaserte tjenester; og kraftforsyning (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 74). Sentralt for å forstå hva som definerer samfunnets funksjonalitet er samfunnets kritiske funksjoner.

Samfunnets kritiske funksjoner, er alle funksjoner som ansees som kritiske, og har både generelle og særegne trekk ved seg. Det mest prominente fellestrekket ved disse funksjonene er betydningen de har for samfunnet (Engen et al., 2016, s. 138). Direktoratet for samfunnssikkerhet og beredskap (2016, s. 8) beskriver kritiske funksjoner med bakgrunn i to faktorer: funksjonen ansees som kritisk dersom bortfall på syv eller færre døgn vil true de grunnleggende behovene til befolkningen; og at beredskapsressursene tilgjengelig vil bli utfordret i dette tidsspennet.

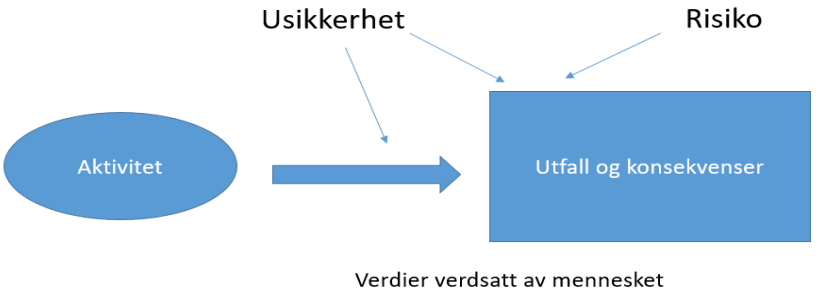
3.1.2 Risikoforståelse og ulike perspektiver

Risiko er et begrep og konsept som det foreligger forskjellige forståelser, og som gjerne tilknyttes samfunn, tradisjoner og fagfelt. Generelt kan en derimot si at risiko brukes for å beskrive «den fare som uønskede hendelse representerer for mennesker, miljø og økonomiske verdier» (Aven, 2006, s. 8).

Den klassiske forståelsen av risiko kan betegnes således *[…] et produkt av sannsynligheten for at en hendelse inntreffer og konsekvensen dersom den inntreffer* (Justis- og beredskapsdepartementet, 2016, s. 28). Definisjonen gir en forståelse av at risiko er noe som handler om fremtiden og dens tilhørende konsekvenser. Sannsynlighet viser til hvorvidt en kan forvente at hendelsen vil inntreffe. Definisjonen er dog noe snever. Usikkerhet, noe som er sentralt ved fastsetting av sannsynlighet er ikke inkludert. Usikkerhet vil alltid være knyttet til fastsettelse av verdier knyttet til sannsynlighet, ergo blir definisjonen mangelfull (Engen et al., 2016, s. 81). Videre inkluderes ikke aktivitet, risikobegrepet blir da ikke heller relatert mot en kontekst og/eller system.

Aven, Boyesen, Njå, Olsen og Sandve (2004, s. 37) legger en annen definisjon til grunn i boken *Samfunnssikkerhet: Risiko er en kombinasjonen av usikkerhet og konsekvens av en gitt aktivitet*. Definisjonen benytter usikkerhet som et mål på vurdering om en hendelse vil inntreffe i en gitt tidsperiode (ibid.). Usikkerhet kan derimot ikke behandles som en størrelse som kan tallfestes på lik linje med sannsynlighet, da usikkerhet favner mye bredere og kan knyttes til informasjon, beregning og andre faktorer. En svakhet ved overnevnte definisjon er at den ikke inkluderer verdier verdsatt av mennesket. Aven et al. (2004) diskuterer dog verdier som mennesket verdsetter. En kan derfor tolke det slik at verdier verdsatt av mennesket ligger implisitt i forståelsen av en «gitt aktivitet». Det er ikke nærliggende å tro at dette er noe lekmenn intuitivt kan tolke, ergo er denne forståelsen også mangelfull. Definisjonen som danner forståelsen for risiko i denne studien favner derfor bredere enn de to eksemplene presentert.

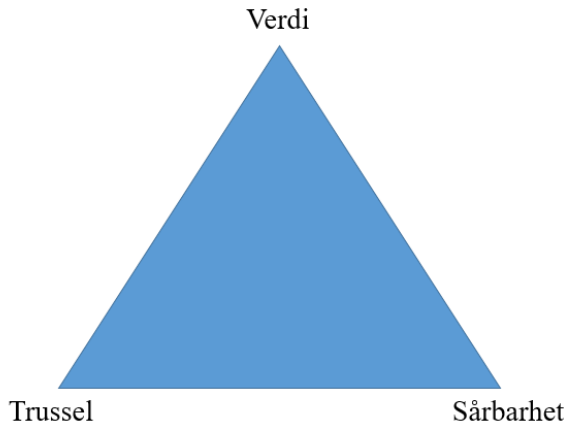
Risiko refererer til usikkerheten om og alvorligheten knyttet til hendelser og konsekvenser av en aktivitet med hensyn til hva mennesket verdsetter (Aven & Renn, 2010, s. 3). En slik definisjon viser til tre aspekter som videre må konkretiseres. Usikkerhet defineres nedenfor. Konsekvenser viser til størrelse, utbredelse, intensitet og omfang av hendelsen. Hva mennesket verdsetter kan variere fra sosiale verdier til materielle verdier og menneskeliv (Engen et al., 2016, s. 81). Figuren 8 illustrerer risikokonseptet visuelt.



Figur 8, Risiko, av Aven og Renn (2010, s. 3)

I overværende definisjon av Aven og Renn (2010, s. 3) vises det til usikkerhet som en sentral variabel. Gitt at usikkerhet er en sentral del av definisjonen av risiko, er det hensiktsmessig å definere begrepet. *Usikkerhet* i denne sammenhengen referer til vanskeligheter ved å forutsi hyppigheten til hendelser og konsekvenser knyttet til dette. Usikkerhet har ofte sammenheng med manglende og/eller feil i datagrunnlaget, endringer i den kausale kjeden eller endringer i kontekst, dårlige målinger, med mer (Aven & Renn, 2010, s. 12). Videre kan en skille mellom aleatorisk og epistemisk usikkerhet, hvorav førstnevnte viser til usikkerhet i resultatene og sistnevnte er knyttet til kunnskapsmangel (ibid., s. 78). Usikkerhet er et sentralt aspekt når endringer forekommer. Disruptiv teknologi forårsaker særlig epistemisk usikkerhet.

Risiko kan også vurderes i henhold til variablene verdi, sårbarhet og trussel, heller enn å vurdere usikkerheten knyttet til hvorvidt en hendelse vil skje. Trefaktormodellen vurderer risiko i henhold til verdi, trussel og sårbarhet. I modellen vektlegges verdi, ergo hva mennesket verdsetter og er avhengig av; sårbarhet, et systems evne til å fungere ved stressituasjoner; og truslene mot systemet. Disse faktorene vektlegges dog ikke likt, og vektingen av faktorene avhenger av hvilket system man ser på (Nasjonal Sikkerhetsmyndighet, 2015, s. 12). Risikoen i samfunnet øker, i henhold modellen, grunnet stadig større kompleksitet og stigende avhengighet av tjenester fra utlandet, sistnevnte som en konsekvens av globalisering (NOU 2016:19, s. 66).



Figur 9, trefaktormodellen. Trefaktormodellen av NSM, Sikkerhetsfaglig råd, 2015 som gjengitt i NOU 2016:19 (s. 44)

Systemrisiko, er et begrep som er diffust og opererer med flere betydninger. Innen finans viser dette til *Risikoen for rystelser i finanssystemet som kan gi alvorlige konsekvenser for realøkonomien* (Finansdepartementet, 2018b, s. 69; Lind, 2016, s. 5). En risiko av slik karakter kan knyttes opp mot manglende finansiell balanse, konsentrasjon og koblinger mellom ulike parter, samt en struktur som belønner risikosøkende atferd i bankene (Finansdepartementet, 2018b, s. 69). Innen samfunnssikkerhet viser begrepet til en hendelse som grenser mellom naturlige hendelser, økonomisk, sosial og teknologisk utvikling, herunder også handlinger drevet av policy (Renn, 2008, s. 5). Hendelsen forekommer gjerne også på et nasjonalt eller internasjonalt nivå, og dermed er slike risikoer også påvirket av globalisering, herunder bredt omfang og berører mange parter (ibid., s. 61). Slike hendelser kan gjerne oppstå en mindre komponent eller et delsystem, men grunnet tette interaksjoner mellom og innad i systemene som vil skape kaskadeeffekter og dermed påvirke hele og i tilfeller andre system (IRGC, 2018, s. 9). Konsekvensene som tillegges slike risikoer kan minne om hva Taleb (2007) ser ved sorte svaner, som vil si store, uventede og ikke-reversible konsekvenser. Systemrisiko kan også være vanskelige å forutse på grunn av at de gjerne er forbundet med kompleksitet, usikkerhet og tvetydighet (Renn, Klinke & Asselt, 2011, s. 234). Studien legger samfunnssikkerhetsforståelsen til grunn når systemrisiko diskuteres.

Karakteristikker knyttet til risiko

Risiko er nå definert og det foreligger en risikoforståelse som favner om både usikkerhet, aktiviteter påtatt av mennesket og en vurdering knyttet til hva mennesket verdsetter. Videre er usikkerhet beskrevet, også forskjellen mellom epistemisk og aleatorisk usikkerhet klargjort, og systemrisiko er blitt definert. Til tross for dette er ikke risikofenomenet beskrevet ferdig. Det foreligger en rekke karakteristikker som kan tillegges en risikoagent. Valget for å beskrive egenskapene falt på Renn (2008) sin kategorisering som skiller mellom lineære, komplekse, usikre og tvetydige risikoer. Grunnen til at en slik kategorisering er foretrukket er av dens generiske form som gjør den anvendelig (Engen et al., 2016, s. 83).

Lineær, risikoer som betegnes som lineære er karakterisert av enkle årsaksforhold, velkjente egenskaper og at de er enkle å analysere og kvantifisere. Sjeldent er slike risikoer grobunn for større problemer som ikke kan løses ved enkle avveiinger eller sammenligning av fordeler og ulemper (Renn, 2008, s. 186). *Usikkerhet,* som allerede poengtert, knyttet til årsaksforholdet og estimatene som er knyttet til risikoagenten. Sentralt for usikkerhet er informasjon: ved økt informasjon om risikoagenten vil en kunne redusere usikkerheten (Renn, 2008, s. 186-187). En skiller gjerne mellom aleatorisk og epistemisk usikkerhet (Aven & Renn, 2010, s. 78), som

redegjort for ovenfor. *Kompleksitet*, knyttet til risiko refererer til et årsaksforhold mellom årsak og konsekvens som er vanskelig å analysere. Her kan ulike bidragsytende faktorer sammenfalle, interagere og påvirke hverandre. Dette kan komplisere den kausale årsakskjeden. I møte med kompleksitet kreves det tilsvarende komplekse analyseverktøy for å avdekke årsakskjeden (Renn, 2008, s. 186). *Tvetydighet*, dette oppstår i de tilfellene hvor det er forskjeller i hvordan aktører oppfatter, vurderer og vektlegger informasjonen en har tilgang på (Renn, 2008, s. 186). En skiller tradisjonelt mellom to former for tvetydighet; fortolkende og normativ tvetydighet. Fortolkende tvetydighet viser til ulike fortolkninger av samme resultat og kan derfor være hva den enkelte ser som relevant (ibid.) Normativ tvetydighet viser derimot til hvilke verdier enkeltpersoner og interessenter verdsetter, herunder vil det gjerne foreligge en diskusjon blant involverte omkring verdiladde problemstillinger (ibid.).

3.1.3 Karakteristikker ved et system

Sårbarhet

Begrepet og konseptet sårbarhet kan inneholde flere aspekter, men generelt kan en si at sårbarhet innebærer et systems evne til å fungere i møte med en risikoagent. Det foreligger dog ulike definisjoner, og i NOU 2000:24 defineres sårbarhet således:

> *Sårbarhet er et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarhet er knyttet opp til mulig tap av verdi. (NOU 2000:24, s. 18)*

I meld. St. 10. 2016-2017 defineres sårbarhet slik:

> *«Manglende evne til å motstå en tilsiktet uønsket handling eller uønsket hendelse, samt manglende evne til å gjenoppta sin funksjon» (Justis- og beredskapsdepartementet, 2016, s. 26).*

Felles for begge definisjoner er at begge understreker at sårbarhet utrykkes som mangler i et system og at dette vil sammen med en uønsket hendelse forårsake at systemet vil har vanskeligheter med å opprettholde og gjenopprette sin funksjon. Definisjonene presentert av Sårbarhetsutvalget (NOU 2000:24) og Justis- og beredskapsdepartementet (2016) omtaler sårbarhet kun i lys av mangler. Det er da nærliggende å tro at de behandler sårbarhet som et fravær og/eller manglende grad av *robusthet*. Om dette faktisk er forholdene er det vanskelig å si noe om, definisjonene blir dog noe misvisende. Dersom både sårbarhet og robusthet brukes om samme et systems evne ville det ikke vært hensiktsmessig å bruke begge begrep i diskusjonen rundt et systems evne til å opprettholde sine funksjoner (Engen et al., 2016, s. 47). Robusthet er egenskaper som designes og/eller tillegges et system med tanke på å

opprettholde systemets funksjon ved en uønsket hendelse, mens sårbarheter er egenskaper som kan bygges opp over lengre tid og være skjult. I så måte vil robusthet være mer proaktivt, mens sårbarheter mer reaktivt (ibid.). Forståelsen for sårbarhet i studien faller derfor nærmere Engen et al. (2016) og Renn (2008). Engen et al. (2016, s. 47) definerer sårbarhet som:

> *Et systems forutsetninger for eller manglende evne til å fungerer under og etter at det utsettes for en uønsket hendelse. (Engen et al., 2016, s. 47)*

Forståelsen sier mer om evnene til systemet, inkludert de manglende, til å håndtere hendelser. Renn (2008, s. 69) vurderer sårbarhet som kvaliteten til et systems evne til å tolerere en uønsket hendelse. Igjen poengteres systemets evne fremfor mangler til å håndtere en hendelse. Videre er det sentralt å se sårbarheter i lys av risikoen en står overfor, noe som gjør sårbarheter dynamiske siden det påvirkes av miljøet rundt systemet. Nye sårbarheter kan oppstå som følge av nye teknologier, økt avhengighet av systemer og økt mobilitet (Renn, 2008, s. 62). Sårbarhet er egenskaper ved et system som gjerne er selvforskyldt, og det foreligger dokumentasjon på at dette er menneskeskapt. Samtidig er det mulig å begrense og redusere sårbarheten ved et system (NOU 2000:24, s. 18).

Outsourcing

Outsourcing også kjent som utkontraktering, for å gi outsourcing en god kontekst er det hensiktsmessig å først klargjøre hvilken betydning som legges i sourcing. Sourcing viser til overførsel av oppgaver/arbeid fra en part til en annen. Outsourcing på sin side defineres av Power et al. (2006, s. 3) som overførsel av oppgaver/arbeid fra en organisasjon til en ekstern tilbyder. I en slik prosess er det identifisert tre komponenter; klienten, de som ønsker oppgaver outsourcet; tjenestetilbyderen som vil overta oppgavene; og oppgavene som outsources av klienten (ibid., s. 4).

Offshoring, er et ganske nærliggende begrep til outsourcing, men skiller seg fra outsourcing ved at det omhandler overførsel til utland. En kan derfor definere offshoring som overførsel av oppgaver som støtter inn- og utlandsaktiviteter til utlandet, enten gjennom interne eller eksterne aktører (Larsen et al., 2013, s. 533).

3.2 Normal Accidents Theory

Bidraget bygger på den teknologiske ekspansjonen samfunnet har undergått, fra pre-industrialisert samfunn til nå å være et post-moderne samfunn. Utviklingen har medført radikale endringer, også i systemene som omringer menneskene. Mye av teknologien rundt i dag oss er potent nok til å skape katastrofer. *Normal Accidents* viser til ulykker som

forekommer i system preget av tette koplinger og komplekse interaksjoner som leder til feil, feil som kan få katastrofale konsekvenser (Perrow, 1999, s. 5). Slike ulykker vil ikke nødvendigvis forekomme hyppig, men de vil forekomme. Systemene er av en slik kompleks natur, noe som skaper iboende egenskaper som medfører systemulykker (ibid.).

Systembeskrivelse

Charles Perrows bidrag synes å være godt egnet til å beskrive systemegenskaper. I følge Perrow (1999, s. 65) kan en inndele et system i fire nivå: del, enhet, delsystem og system. En del er det laveste nivået i systemet, dette kan inkludere deler som er nødvendig for gjennomføring av en prosess. Enhet viser til et sett med deler som sammen utgjør en enhet (ibid.). Et delsystem utgjøres av en rekke enheter som sammen tjener en felles funksjon. Delsystemene danner sammen systemet (Perrow, 1999). Inndelingen av nivåene er sentralt for å vurdere hva som betegner og skiller en ulykke fra komponentfeil. En slik nivåinndeling gir også bedre systemforståelse og dermed et enklere analyseverktøy. Tett knyttet til nivåinndelingen av systemet for betalingsformidling er forståelsen av ulykker. Perrow (1999, s. 66) hevder at dersom det forekommer skader ved systemnivåene del eller enhet, er dette å ansees som hendelser. Dersom skader forekommer på nivåene delsystem eller system vil dette være ulykker.

Koplinger

Et system har mellom sine ulike deler trekk ved seg som preger dens oppbygning og egenskaper. Koplinger beskriver hvordan operasjoner er koplet sammen i et system. Dette brukes for å beskrive avhengigheten operasjonene har av hverandre (Engen et al., 2016, s. 144). Avhengigheten avhenger av hvorvidt en har et løst eller tett koplet system.

Et løst koplet system vil ikke nødvendigvis ha mange tidsavhengige prosesser, og sluttproduktet i slike system vil ikke ødelegges eller endres ved forsinkelser. Tett koplede system er derimot avhengig av tid, her kan ikke prosessen forsinkes da dette vil innvirke på produksjonen (Perrow, 1999, s. 93). En annen karakteristikk som skiller løst og tett koplede systemer er rekkefølgen på prosessene. I løst koplede system er ikke rekkefølgen på prosessene sentralt for sluttproduktet. Ved tett koplede system foreligger det derimot en bestem rekkefølge som er vanskelig å avvike fra i produksjonen, A må komme før B (ibid.). Et ytterligere trekk ved tett koplede systemer er systemdesignen. Systemet i tett koplede system er designet på en slik måte at det er kun én produksjonsform som skaper et ferdig produkt. I et løst koplet system så er det derimot flere ulike måter en kan produsere endeproduktet, dette åpner for forskjellige «utveier» i produksjonen (ibid., s. 94). Ressursene

og komponentene er også noe som skiller løst og tett koplede systemer. I løst koplede systemer kan komponenter og ressurser utnyttes feil og ødelagt uten at dette medfører store konsekvenser. I systemer som er tett koplede er det ikke rom for dette, ressursene og komponentene som utgjør systemet må utnyttes på en korrekt måte og utstyret er vanskelig erstattet (ibid.). I løst koplede systemer er det mer rom for navigering ved hendelser. I tett koplede systemer er ofte løsningene for å håndtere slike hendelser bygget inn i systemet (ibid., s. 95).

Interaksjoner

Interaksjoner er noe som preger ens hverdag og dette er noen en tar del i hver dag. Innen systemer er det også interaksjoner mellom de ulike deler, enhet, delsystem eller system. Samspillet mellom disse kan beskrives som lineære eller komplekse (Perrow, 1999, s. 72). System med *lineære interaksjoner* kjennetegnes ved deres simpelhet. Kjente produksjonssløyfer og –sammenhenger, segregerte prosesser som følger hverandre, komponentene tjener ett formål og er enkle å erstatte (ibid., s. 72,75). I systemer med slike karakteristikker er det enkelt å hente ut informasjon ved avvik eller ulykker i systemet. Dette er mulig da interaksjonene mellom komponentene er lineære og legger opp til enkel informasjonsuthenting (ibid., s. 78).

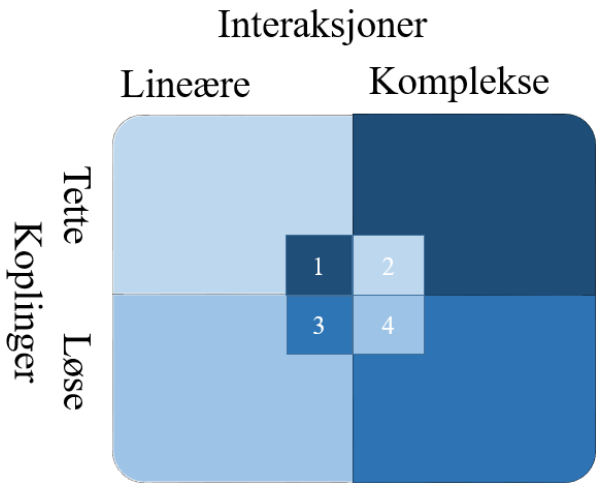
Komplekse interaksjoner, er som betegnelsen indikerer komplekse – mindre tydelig interaksjonsmønster. Interaksjonene blir komplekse grunnet en rekke forhold som nærhet mellom komponentene, komponentene tjener flere funksjoner og at det er tilbakeføringssløyfer (Perrow, 1999, s. 75-76). Disse faktorene kan medføre at interaksjonene mellom ulike deler, enheter og delsystem kan være utenfor hva delene hva tiltenkt i designfasen av systemet. De ulike komponentene som utgjør systemet vil også være mindre segregerte om de tjener flere funksjoner – dette vil også skape økt nærhet til andre komponenter utenfor ens egne delsystem. Eksempelvis kan dette forklares slik: skade på komponent A i system Z kan få utslag i komponent B i system Z, men også C i system X, ettersom komponent A tjener en funksjon som både komponent B og C trenger for produksjon.

Perrow (1999, s. 78) er påpasselig med å understreke at de fleste system er designet med lineære deler, ergo preges de fleste systemer av lineære interaksjoner. Systemene kan dog også ha komplekse interaksjoner, grunnet selv det mest lineære systemet vil til tider ha komplekse interaksjoner (ibid.). Videre vil det i systemer også foreligge interaksjoner som ikke er kjente og fremstår som *skjulte interaksjoner.* Interaksjoner av en slik natur oppfattes

ikke av de som opererer i systemet og er derfor vanskelig å avdekke. Systemavgrensing er heller ikke noe som nødvendigvis begrenser omfanget på interaksjonene. Deler i ulike delsystem kan derfor interagere med hverandre uten vår viten (ibid., s. 79).

Modell for karakterisering av systemer

Dimensjonene koplinger og interaksjoner har dannet grunnlaget for utviklingen av modellen som kan benyttes til å klassifisere systemer. Interaksjoner og koplinger sier noe om hvilke forhold som preger systemet. Modellen differensierer ikke mellom aktiviteter i systemene, så ulike systemer kan kategoriseres ut fra denne modellen (Perrow, 1999, s. 98). Systemer med både komplekse interaksjoner og tette koplinger har ifølge Perrow har potensiale for *Normal Accidents* (Engen et al., 2016, s. 146). Slike systemer har, i de mest fremtredende eksemplene presentert av Perrow, aktiviteter som har store ringvirkninger utover sitt opprinnelige virke. Ergo vil ulykker i slike system kunne forårsake negative konsekvenser for første-, andre-, tredje- og fjerdeparts ofre. Figur 10 illustrerer modellen i henhold til dimensjonene koplinger og interaksjoner. Et sentralt aspekt ved å vurdere systemer fra disse dimensjonene, er at dette ikke viser et statisk bilde. System, som alt annet, vil oppleve forandringer (Engen et al., 2016, s. 146).



Figur 10, Perrow's klassifisering av systemer

Perrows syn på finanssektoren

Perrow (1999) poengterer hvordan finanssektoren har blitt mer kompleks, særlig med tanke på at aktivitetene i sektoren er mer grensekryssende enn tidligere (s. 385). Sentralt ved globaliseringen av finansielle aktiviteter er at alle lover, reguleringer, standardiseringer og systemer må være kjent for aktørene som deltar i aktivitetene. En kan da snakke om et nett av multiple faktorer som interagerer med hverandre og innvirker på hverandre (ibid.). Samtidig vil det økte transaksjonsvolumet i finanssektoren kunne medføre tettere koplinger da den løpende risikoen knyttet til oppgjør vil være større. Utbredelsen av derivater og valuta vurderes til å skape kompleksitet og tette koplinger i systemet, særlig knyttet til utbredelsen av markedet og tilhørende kommunikasjonskanaler (ibid.). Systemet vurderes dog ikke til å være preget av *Normal Accidents* på lik linje med andre systemer, ettersom atferd hos en

rekke aktører skaper økt kompleksitet og tette koplinger, ergo så er ikke systemulykker uunngåelig. Egenskapene er dermed ikke iboende i systemet, men heller tilført og kan så også fjernes – om en vil nok (ibid., s. 387). Trekkene Perrow (1999) presenterer kan en også se igjen i systemet for betalingsformidling, men her har utviklingen knyttet til samordning og standardisering kanskje fjernet noe av kompleksiteten mellom komponentene. Denne trenden kan derimot bli utfordret av et nytt og mer internasjonalt aktørbilde for betalingsformidlingen.

3.3 Organisatoriske ulykker

Organisatoriske ulykker karakteriseres av James Reason (1997, s. 1) som hendelser med sjelden forekomst men med et katastrofalt potensial. Hendelser av slikt omfang oppstår gjerne i systemer og organisasjoner som opererer innen komplekse moderne teknologier. Ulykkene har ofte multiple årsaker, og lang kausalkjede som involverer en rekke ulike nivå, komponenter, personell og selskap. Av denne årsak er slike hendelser vanskelig å forutse. Rammede i slike ulykker begrenses ikke kun de nærmest systemet, men kan også ha konsekvenser for ikke-involverte tredje- og fjerdeparter (ibid.). Tredjeparter viser til personer uten tilknytning til systemet og fjerdeparter viser til fremtidige generasjoner. Perspektivet på ulykker er noe han deler med Perrow (1999), de skilles derimot i spørsmålet på om det er mulig å forhindre. Hvorav Perrow (1999) har et deterministisk og pessimistisk syn på aktiviteter som kan medføre systemulykker, er Reason (1997) noe mer positiv. Latente betingelser og aktive feil er sentralt for å forstå årsaker knyttet til organisatoriske ulykker. Til tross for at latente forhold og aktive feil er grunnpilarer i synet på organisatoriske ulykker, vektlegges samtidig en rekke faktorer som innvirker og skaper disse. Faktorene inkludert er de som oppfattes som relevant for betalingsformidlingen.

3.3.1 Aktive feil og latente forhold

Reason (1997, s. 10) peker på hvordan organisatoriske ulykker kan oppstå. Særlig to faktorer presenteres som årsaker til utviklingen av slike ulykker, aktive feil og latente forhold. *Aktive feil* er den menneskelige faktoren som er mest synlig og ergo enkelt å avdekke. Disse feilene begås i den «skarpe enden», altså der operasjonene gjennomføres og kan enkelt spores til den enkelte operatør eller bruker (ibid.). Slike feil kan også i flere tilfeller tilskrives som en konsekvens av latente forhold som er iboende i organisasjoner.

Latente forhold viser på sin side til svakheter i en organisasjon som kan være tilstedeværende i flere år uten at en større hendelse oppstår. Forholdene kan skapes ved design av et system, vedlikehold, dårlig utstyr, aktive feil, med mer. Fremveksten av latente forhold er gjerne

knyttet til avgjørelser tatt på et høyt hierarkisk nivå (Reason, 1997, s. 10). En av de større problemene knyttet til latente forhold er identifisering og eliminering av latente forhold. De kan være tilstede i en organisasjon i en årrekke og kunne bli trigget av et skift i miljøet rundt, latente forhold er i så måte en uunngåelig faktor knyttet til organisasjonsstruktur (ibid., s. 11).

Det foreligger to sentrale skiller mellom aktive feil og latente forhold. Hvor førstnevnte ofte har umiddelbare og kortsiktige effekter på systemet, er latente forhold iboende i systemet over lengre tid og er ikke en faktor frem til endringer i omgivelsene gir dem evnen til å svekke barrierene (Reason, 1997, s. 11). Det andre skillet ligger i hvor årsaken til oppstår. Aktive feil gjøres gjerne i den skarpe enden, mens årsaken til latente forhold gjerne oppstår ved avgjørelser fattet på et høyere nivå (ibid.).

Automatisering og outsourcing

Automatisering er en tematikk som Reason vier mye plass til i boken *Managing the risks of Organizational Accidents.* Han ser særlig en problematikk knyttet til hvordan automatisering kan bidra til at et system vil kunne feile. Listen er lang men av viktighet er faktorer som: dårligere informasjonsflyt, det kan skjule interessante hendelser, forandringer og avvik, økt kompleksitet gjennom design og produksjonsmåte, tilgjengeliggjøring av viktig og sensitiv informasjon på flere nivå (Reason, 1997, s. 46). Kunnskap er i tillegg et sentralt aspekt som ofte forsvinner grunnet at oppgavene overtas av andre. Problematikken identifisert ved automatisering kan overføres til outsourcing. Spesielt vil kompleksiteten i systemet øke ved offshoring (Larsen et al., 2013, s. 535). En videre konsekvens av økt kompleksitet, noe som kan medføre at verdikjeden blir uoversiktlig og flere verdikjeder oppstår (ibid.). Bankene blir derfor sittende med å styre flere parallelle verdikjeder for å kunne håndtere alle sine aktiviteter (ibid.). Videre vil organisasjonene som outsourcer ha mindre kontroll over oppgavene. Samtidig er også kunnskap noe som kan bortfalle ved outsourcing og offshoring da andre aktører overtar oppgaver tidligere holdt av organisasjonen.

Farlige forsvar

Forsvar og barrierer er egenskaper som de fleste systemer behøver for å kunne beholde sin funksjon under stressituasjoner. Systemer med barrierer og forsvar har uten tvil blitt sikrere mot truslene barrierene var designet for å beskytte mot. Barrierene har likevel paradoksalt presentert nye risikoer ovenfor systemet, særlig i grensen mellom mennesket og teknologi – det er dette som er tenkt som farlige forsvar. Her presenteres det ulike trekk ved barrierer som kan skape problemer i et system. Fokuset ved bidraget ligger ikke på barrierenes funksjon, men heller de ulike fallgruvene som kan skape latente forhold. Barrierer og dets funksjon

presenteres i dybden i 3.4. Generelt kan en si at sikkerhetstiltak og nye barrierer bidrar til å øke kompleksiteten ved et system da disse også utgjør komponenter i systemet (Reason, 1997, s. 59). Reguleringer som sikter på å begrense sannsynligheten for menneskelige feil i systemet kan også gjøre systemet mer utsatt for ulykker. En slik vurdering kan tillegges reguleringer, da det kan begrense operatørenes evne til å handle dersom systemet faller utenfor normalsituasjon eller i ekstreme tilfeller også ved normalsituasjon (Reason, 1997, s. 49). Samtidig vil det være tilfeller hvor operatører opererer utenfor tillatte grenser for at systemet skal kunne opprettholde drift. Dette kan medføre økt sannsynlighet for feil senere og sannsynligheten for at feilen vil ha negativt utfall (ibid., s. 51).

Konseptet om *forsvar i dybden*, ytterligere presentert i kapittel 3.4.2, presenter hvordan barrierer sammen forhindrer en hendelse i å forekomme. Konseptet illustreres gjerne på som en lineær kausal rekke, hvor en barriere følger den neste (Reason, 1997, s. 54). En slik illustrasjon som viser redundans kan være misvisende da interaksjoner og kaskadeeffekt mellom komponenter ikke vurderes. En kan også argumentere for at forsvar i dybden vil bidra i å skjule hendelser fra operatøren, noe som kan bygge opp latente forhold. Dette er også en faktor som kan svekke operatørenes læring, da de ikke får øvelse i å rette opp feil i systemet (ibid., s. 55). En annen bidragsytende faktor er varslinger. Varslingssystemer kan ha feil ved seg som medfører varslinger i normalsituasjoner. Dette kan skape en pessimistisk holdning til varslingene, og at en ikke agerer når varslingene stemmer med situasjonen (Reason, 1997, s. 56-57). En kan se paralleller til Aesops fabler og «Gutten som ropte ulv», varslingssystemet blir da en faktor som svekker systemet og et irritasjonsmoment for operatørene (ibid.).

3.4 Barrierer

Barrierer brukes i denne sammenhengen vekselsvis med forsvar da forståelsen i denne studien er at de tjener samme funksjon. Av kapittel 3.1.3 kan en forstå at det foreligger en rekke definisjoner og forståelser av barrierer, deres design og funksjon. Forståelsen av barrierer belager seg på karakteristikk fra Hollnagel (2004, s. 68). Karakteristikken beskriver barrierer som en hindring som kan innvirke på hvorvidt en uønsket hendelse inntreffer og konsekvensene ved uønskede hendelser (ibid.).

I boken *Managing the Risks of Organzational Hazards* presenterer James Reason sine tanker om hvilke funksjoner forsvar skal tjene. I følge Reason skal forsvar tjene én eller flere av følgende funksjoner: etablere forståelse og bevissthet om farer; gi tydelig veiledning i sikker opptreden; alarmere og varsle når fare er til stede; gjenetablere sikkerhet når systemet

kommer i en unormal situasjon; sette inn sikkerhetsbarrierer mellom farer og potensielle tap; lukke inn og eliminere farer dersom de skulle bryte gjennom barrierer; sikre rømning og redning dersom innelukking/eliminasjon av hendelser mislykkes. Sentralt i denne opplistingen er tanken om forsvar i dybden (Reason, 1997, s. 7), konseptet redegjøres nedenfor i kapittel 3.4.2. Forsvar i dybden karakteriseres gjerne av forsvar med ulike funksjoner og utforming, en kan skille mellom myke, harde, forhindrende, beskyttende aktive og passive barrierer.

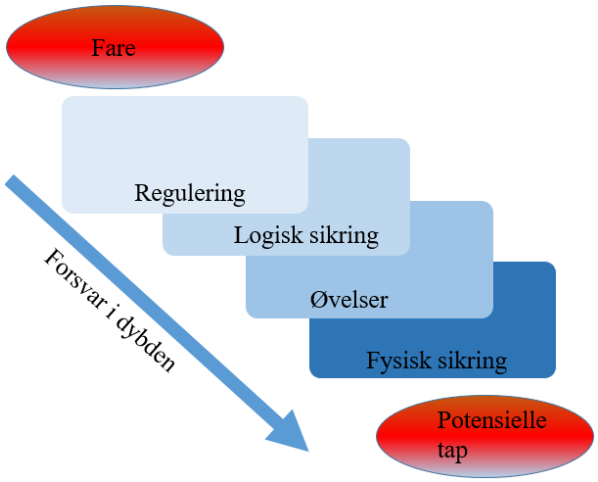
3.4.1 Ulike barrierer

Barrierer kan ha ulike funksjoner og kjennetegn, mange har definert barrierer med fokus på disse kjennetegnene som skiller (Aven et al., 2004; Hollnagel, 2004; Kjellén, 2000; Reason, 1997). Studien tar utgangspunkt i Hollnagel (2004) og hans beskrivelse, som er: en hindring som kan innvirke på hvorvidt en uønsket hendelse inntreffer og konsekvensene ved uønskede hendelser (s. 68). Hensikten med å benytte en slik generisk definisjon av barrierer er hovedsakelig knyttet til alle de forskjellige formene barrierer kan i henhold til hvilket system som vurderes. I definisjonen fra Hollnagel (2004, s. 68) legges det ikke føringer for hvilke egenskaper som inkluderes for å beskrive barrierer, ergo blir vurderingen for hva som ansees som barrierer kontekstualisert. Skillet på barrierer som presenteres nå er ikke gjensidig utelukkende, men heller overlappende siden differensieringen baseres på ulike egenskaper knyttet til barrierer.

Myke barrierer er en kombinasjon av papirer og mennesker. Typiske eksempler på relevante papirer knyttet til myke barrierer er lovgivning, regler, regulering og prosedyrer. Det menneskelige bidraget kan en vurdere som regulering/kontroll, trening, drilling, briefing og administrativ kontroll (Reason, 1997, s. 8). *Harde barrierer* inkluderer teknisk utsyr utformet for sikkerhet, fysiske barrierer, alarmer og varsling, konstruerte sårbarheter ved systemet, systemforbedringer og systemgrenser (ibid., s. 8). *Passive barrierer* viser til barrierer som er uavhengig aktivering fra eksternt hold. Barrierene er tilstede uavhengig situasjon og kontekst, slike barrierer er gjerne designet inn i systemet (Aven et al., 2004, s. 122; Kjellén, 2000, s. 86). *Aktive barrierer* på sin side krever en aktivering for å kunne fungere, dette kan skje enten automatisk, eksternt eller ved en manuell operasjon (Aven et al., 2004, s. 122). Slike barrierer kan i større grad enn passive barrierer være sårbare ovenfor atferd knyttet til mennesket og systemet (Kjellén, 2000, s. 86). Hollnagel (2004, s. 68) presenterer ett ytterligere skille, her skilles det mellom forhindrende og beskyttende barrierer. *Forhindrende barrierer* er designet med tanke på å forhindre at uønskede hendelser skal oppstå. *Beskyttende barrierer* er designet med sikte på å minimere konsekvensene ved fremkomsten av uønskede hendelser (ibid.).

3.4.2 Forsvar i dybden

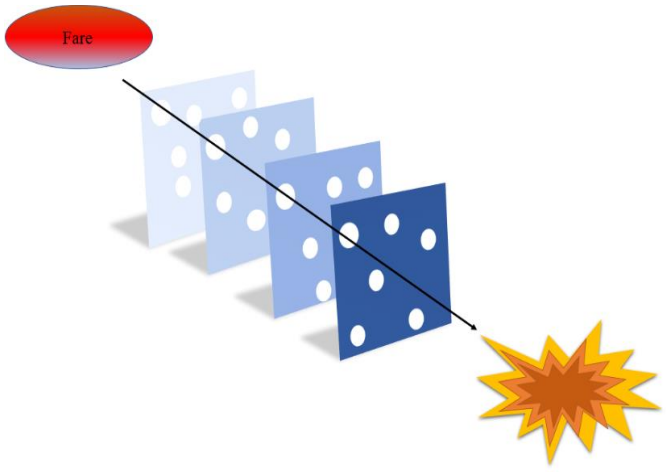
Konseptet viser til hvordan bruk av barrierer kan forhindre uønskede hendelser å skje. Konseptet er særlig relevant i forhold til organisatoriske ulykker som gjerne omhandler organisasjoner i store og komplekse system. Lagvis bruk av barrierer kan sammen forhindre ulykker å skje. En slik lagvis bruk av barrierer kan skape redundans i systemets sikkerhet. Barrierene er en kombinasjon av ulike typer barrierer som sammen beskytter ulike deler av systemet.



Figur 11, forsvar i dybden

Konseptet om forsvar i dybden beskrives som både en velsignelse og en forbannelse. Forsvar i dybden medfører gjerne økt kompleksitet i systemene ettersom dette øker antall komponenter i systemet (Reason, 1997, s. 8). Bruk av flere barrierer kan også medføre en fremmedgjøring for de som opererer systemet da en i større grad blir fjernet fra operasjonen. En slik fremmedgjøring kan medføre en oppbygning av latente forhold som påpekt i kapittel 3.3.1.

Barrierene en benytter seg av er sjeldent uten mangler og kan gjerne ha feil ved seg, noe som muliggjør potensialet for manifestering av større ulykker. Dette illustreres godt av figur 13 som er en gjenskapelse av sveitserostmodellen (Reason, 1997, s. 9). Modellen må sees som dynamisk hvor de ulike barrierene beveger seg inn og ut av banen for faren. Disse «bevegelsene» er mye grunnet eksterne forhold som påvirker konteksten for risikobildet. Med dette menes at sårbarhetene kan variere ut fra omringende miljø og hvilken kontekst system befinner seg. I hver barriere beveger også hullene seg (ibid.). Hullene kan sees som både latente forhold og aktive feil.



Figur 12, Sveitserostmodellen

3.5 Prinsipp for samfunnssikkerhetsarbeid

Stortingsmelding 17. 2001-2002 presenterte tre prinsipp for arbeid mot styrket samfunnssikkerhet (Justis- og politidepartmentet, 2002, s. 4) Ansvars-, likhets- og nærhetsprinsippet var lenge de ledende prinsippene for samfunnssikkerhets- og beredskapsarbeid (Justis- og beredskapsdepartementet, 2012, s. 39). Til tross for at prinsippene fungerte, åpnet de ikke for kommunikasjon og samordning mellom aktører involvert i arbeidet. Samvirkeprinsippet ble derfor presentert for å sikre dette (ibid.). Prinsippene er hensiktsmessige særlig i henhold til hvordan nye aktører kan påvirke myndighetenes og bedriftenes evne til å utføre sikkerhets- og beredskapsarbeidet.

Ansvarsprinsippet tilsier at den som har ansvar i normalsituasjon også har ansvaret hvor det forekommer ekstraordinære situasjoner (Justis- og politidepartmentet, 2002, s. 4). Innunder dette skal også ansvarlig etat, myndighet eller virksomhet også ha ansvaret for beredskapsforberedelser. Her skal det planlegges hvordan funksjoner i ens egne ansvarsområde skal kunne opprettholde og eventuelt videreføres ved en ekstraordinær hendelse (Engen et al., 2016, s. 282; Justis- og beredskapsdepartementet, 2012, s. 39).

Likhetsprinsippet bygger oppunder ansvarsprinsippet, nemlig at ansvaret ikke endres ved krisesituasjon og –håndtering (Engen et al., 2016, s. 283). Organisasjonen i krisesituasjon skal i denne sammenheng være så lik organisasjon man opererer med til daglig (Justis- og beredskapsdepartementet, 2012, s. 39; Justis- og politidepartmentet, 2002, s. 4)

Nærhetsprinsippet påpeker at håndteringen av krisesituasjoner skal skje på lavest muligste nivå (Justis- og politidepartmentet, 2002, s. 4). De som er nærmest krisesituasjonen er gjerne de som egner seg best til å håndtere den. Prinsippet bygger oppunder ansvarsprinsippet, dersom en krise oppstår innenfor ens mandat er det etat, myndighet, organisasjonen eller virksomhetens ansvar å håndtere denne (Engen et al., 2016, s. 283).

Samvirkeprinsippet introdusert i 2012, peker på at aktører som er ansvarlig for et virke selv må sikre samvirke og samordning med relevante aktører i forebygging-, beredskap- og krisehåndteringsarbeidet (Justis- og beredskapsdepartementet, 2012, s. 39). Prinsippet tydeliggjør behovet aktørene har i å kartlegge avhengigheter, på alle nivå, og hvilke aktører nødvendig for forebyggende og beredskapsarbeid (ibid.).

4. Metodisk fremgangsmåte

I dette kapittelet beskrives studiens vitenskapelig ståsted, forskningsdesign, hvordan empirien er generert, ulike tankekors knyttet valg, studiens validitet og reliabilitet samt etiske utfordringer.

4.1 Forskningsstrategi og -design

Oppgavens ontologiske perspektiv er i utgangspunktet tett knyttet opp mot positivisme. Det eksisterende systemet for betalingsformidling tas i så måte som en gitt variabel, som gjennom empiriske observasjoner kan analyseres. Samtidig kan en ikke si at perspektivet bevares i vanntett skott, den epistemologiske tilnærmingen har trekk både forskeren og leseren må identifisere. Ved bruk av kvalitativ metode og semistrukturerte intervju søker vi kunnskap fra informantene og deres ståsted, en metodologi som er grunnleggende fenomenologisk (Tjora, 2012, s. 105). Metodologiske tilnærminger som fenomenologi er hensiktsmessig da det gir tilgang til representanter med kunnskap om systemet og de nåværende endringene. Samtidig benyttes dokumentstudier som datagenering, noe som også ansees som kvalitativ metode (ibid., s. 105)

Strategi

Målet med oppgaven er å undersøke hvilken effekt nye aktører inn i verdikjeden for betalingsformidling vil ha for samfunnssikkerheten. De nye aktørene, særlig fintechs og bigtechs, representerer nye fenomen hvor det ikke foreligger mye dokumentasjon. En kvalitativ tilnærming er derfor hensiktsmessig, da dette fremhever innsikt og søker forståelse, hvor den kvantitative tilnærmingen fremhever oversikt og søker forklaring (Tjora, 2012, s. 22). I tillegg til egen datainnsamling, er det en rekke dokumenter som er supplert for å besvare forskningsspørsmålene. Dokumentene har visst seg hensiktsmessig i å gi et overordnet bilde av forholdene i norsk betalingsformidling. Studien er utviklet med en abduktiv tilnærming, med et iterativt preg. I startfasen med kartlegging av potensielle vinklinger, var preget av en prosess preget av mye informasjonsinnhenting. Informasjonen ble innhentet og vurdert opp mot potensielle teoretiske bidrag, dette er karakteristikk bruk til å beskrive den abduktive tilnærmingen (Tjora, 2012, s. 26). Det iterative preget skyldes hvordan tidlig empiriinnsamling har preget utformingen av oppgaven, dette har medført at endringer har forløpt.

Design

Studien er designet som en unik casestudie, et slikt design fokuserer på det spesifikke ved casen (Ringdal, 2013, s. 171). Designet er passende gitt den unike utformingen det norske betalingssystemet har (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 83; NOU 2015:13, s. 168). Norsk betalingsformidlings utforming forsvarer et slikt design, det foreligger ingen andre systemer for betalingsformidling, kanskje utenom Danmark, som ligner det norske. Dette kunne åpnet for en komparativ studie av disse betalingssystemene, men grunnet tilgjengelighet, ressurser og tid er ikke gjort. Videre vil en unik casestudie prøve å fange kompleksiteten knyttet til systemet som analyseres og det unike (Ringdal, 2013, s. 108). Sådan vil dette åpne for en analyse av hvilken innvirkning nye aktører har på norsk betalingsformidling.

Videre er det hensiktsmessig å forklare for leseren at studiens forskningsspørsmål 1 og 2 er besvart med utelukkende empiri. Årsaken til dette er knyttet til naturen av forskningsspørsmål 1 og 2, deres utforming krever ikke nødvendigvis noen form for bruk av teoretiske bidrag. Det at de da besvares kan forsvares utelukkende grunnet at teoretiske bidrag i denne situasjonen ville ikke inkludert noen vesentlige verdifulle bidrag for analysen. Studiens omfatning er også til dels årsak til dette, da den allerede overskrider anbefalt lengde. Ytterligere analyse av forskningsspørsmål 1 og 2 ville medført vesentlig større antall sider.

4.2 Forskningsprosess

Prosessen med utvikling av oppgaven ble påbegynt i oktober 2018 hvor ulike mulige tema ble vurdert. Det ble sendt ut en skisse til Bits AS, herfra ble det utviklet en skisse hvor begge parter hadde input til problemstilling, tematikk og samarbeid. Fra januar 2019 ble jeg tildelt en veileder fra Universitetet i Stavanger og en veileder hos Bits AS. Kort tid etter tildeling av veileder ble det gjennomført veiledning med veileder fra Universitetet i Stavanger, her ble det påbegynt en prosess med å utvikle forskningsspørsmål som støtter oppunder problemstillingen. Problemstillingen ble også presisert.

Store deler av januar, februar og deler mars ble brukt til en pilotstudie for å få oversikt over de sentrale delene og den historiske konteksten for betalingsformidling i Norge. Deler av pilotstudien er inkludert i systembeskrivelsen i kapitel 2, pilotstudien i sin helhet ligger i vedlegg 6. Samtidig ble det teoretisk grunnlaget utarbeidet, grunnlaget som ble utarbeidet favnet bredt i søken etter å kunne besvare forskningsspørsmålene. Dette bærer preg av en iterativ tilnærming, med dette så menes det at teorigrunnlaget benyttet har kontinuerlig blitt

vurdert mot nye empiriske funn. Det ble samtidig i februar konsultert med veilederne fra både Universitet i Stavanger og Bits AS.

I fellesskap med veileder fra Bits AS ble potensielle informanter diskutert. Veileder fra Bits AS formidlet i begynnelsen av april en liste med potensielle informanter, som deretter ble kontaktet for fastsettelse av dato for intervju. I midten av april ble det gjennomført et møte hos kontorene til Bits AS hvor jeg fikk tildelt informasjon knyttet til betalingsformidling og interbanksystemet, samt regler knyttet til «Blåboka».

Gjennomføring av intervju ble påbegynt i slutten av april, det var tenkt å gjennomføre alle intervjuene på 3 uker. Gjennomføringen av intervjuene ble som etter planen gjennomført på tre uker og var ferdig i midten av mai. Fremstillingen av empirien, både primær og sekundærdata ble påbegynt i slutten av april. I mai ble analysen av resultatene påbegynt og den påfølgende analysen ble gjennomført i juni.

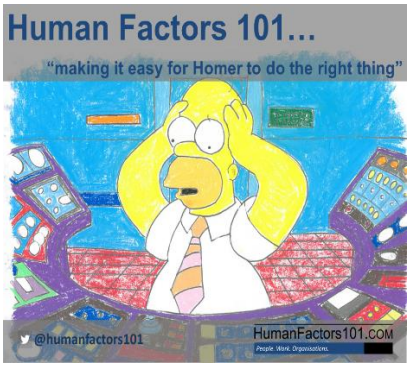
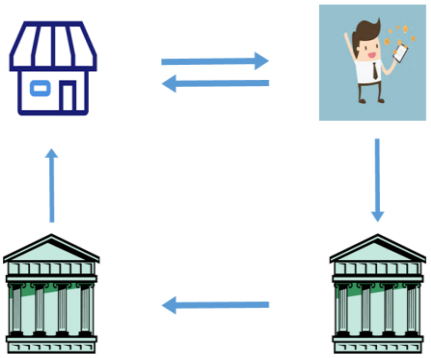
4.3 Innsamling av data

4.3.1 Primær og sekundærdata

Primærdata kan betegnes som alle data samlet inn eller planlagt innsamlet av forskeren for prosjektets formål (Ringdal, 2013, s. 117). Studien belager seg på primærdata, i form av semistrukturerte intervju. Det er gjennomført 5 intervju med ulike aktører innen betalingsformidlingen. Empirien generert fra disse intervjuene presenteres i kapittel 5.1 og 5.2 og der sett i relasjon til forskningsspørsmål 1 og 2. Primærdataen er ment å belyse hvordan sikkerheten i betalingsformidlingen er, samt hvordan de ulike aktørene jobber for å opprettholde sikkerhet. Deltakende informantene er alle aktører innen norsk betalingsformidling, se kapittel 4.3.4 for utvalg av informanter.

Sekundærdata kjennetegnes ved at det allerede foreligger og er tilgjengelig for forskeren (Ringdal, 2013, s. 112). Avgrensningen for hva som er sekundærdata er vid, datagrunnlaget en har tilgjengelig er derfor omfattende. Slik data er hensiktsmessig til å beskrive historiske hendelser og se endring over tid (ibid.). Denne oppgaven har benyttet seg av rapporter, finansmarkedsmeldinger, NOUer, ROS-analyser, lover, regler, reguleringer og bøker som både empiri knyttet til forskningsspørsmålene men også i systembeskrivelsen. Nyhetsartikler er også benyttet for å vise det aktuelle bildet knyttet til endringer i betalingstjenester i Norge, særlig knyttet til nye aktører. Sekundærdataen ble i større grad benyttet for å supplere og en bredere forståelse knyttet til betalingsinfrastrukturen, dets sårbarheter, trusler og aktualitetsbilde.

Tabell 3, oversikt over teoretiske og empiriske bidrag

<table>
<tr><th>Menneskelige faktorer</th><th>Teknologiske faktorer</th><th>Organisatoriske faktorer</th></tr>
<tr><td> 
</td><td>  </td><td>  </td></tr>
<tr><td>Forståelse
Holdning
Vurdering
Kompetanse</td><td><u>Teorier:</u>
Barrierer
Normal Accidents.
Organisatoriske ulykker.
Samfunnssikkerhets– og beredskapsarbeidsprinsipp</td><td>Utvikling
Open Banking
PSD2</td><td><u>Rapporter, lovverk & teori:</u>
PSD2
Evry
NOU
Perrow</td><td>Reguleringer og regler
Ansvarsforhold
Sårbarheter</td><td><u>Bidrag:</u>
Norges Bank
Bits AS – “Blåboka”
NOU
ROS-analyser
Aven
Reason
EBA</td></tr>
</table>

4.3.2 Intervjuguider

Innsamlingen har jf. kapittel 4.3.1 blitt gjort ved et semistrukturert intervju. Semistrukturert intervju brukes av flere vekselvis med dybdeintervju. Intervjuformen bruker åpne spørsmål, dette åpner for at informantene kan utdype sine utsagn og digresjoner (Tjora, 2012, s. 105). Rom for fordypning og digresjoner går til viss grad på bekostning av å finne kunnskap om det spesifikke. Etter utviklingen av intervjuguidene ble de sett igjennom, endret og ferdigstilt med input fra veiledere. Deler av intervjuguidene er utviklet og tilpasset til informantene for å be avdekke informantens perspektiv. Samtidig er det noen spørsmål som er felles for flere intervjuguider. Forskningsspørsmålene er også ved tilfeller blitt benyttet som intervjuspørsmål, dette viste seg hensiktsmessig da spørsmålene er formulert som åpne spørsmål. Forskningsspørsmålene gjorde det mulig for informantene til å gå i dybden. Intervjuguidene var en ledende samtalestarter ved intervjuene, dog ble ikke alle spørsmålene nødvendigvis gjennomgått ved alle intervju, mer om dette i kapittel 4.3.3. Intervjuguidene presenteres i vedlegg 2,3,4 og 5.

4.3.3 Gjennomføring av intervjuer

I forkant av intervjuene ble det sendt ut informasjonsskriv, begrepsliste og intervjuguide til informantene. Informasjonsskrivet formidlet informasjon om hensikten med intervjuene, forespørsel om båndopptak av intervjuene og kontaktinformasjon til intervjuer, se vedlegg 1. Begrepslisten ble lagt ved for at informantene og intervjuet skulle ha en felles forståelse knyttet til ulike begreper som benyttes innen finans- og samfunnssikkerhetsarbeid, se vedlegg 2. Intervjuguidene ble formidlet til informantene en dag før planlagt intervju, det ble ansett som hensiktsmessig å formidle denne i forkant av intervjuet for å gi informantene tid til å forberede seg. Om informantene faktisk forberedte seg gjennom å lese begrepsliste og intervjuguide er det lite grunnlag for å vurdere.

Alle intervjuene, utenom ett, ble gjennomført enten over telefon eller via Skype, dette grunnes hovedsakelig med årsaker som økonomi, ressurser og tid. En fordel med denne intervjuformen er at informantene kan ha en betryggende følelse med tanke på anonymitet. Samtidig behøver ikke informantene å være bevisste over at de blir tatt opp, som en kan ved synet av en båndopptaker (Tjora, 2012, s. 141). En ulempe ved at intervjuene ikke ble gjennomført ansikt-til-ansikt er at samtaleaspektet faller bort, herunder kroppsspråk og at det blir mer formelt. Konsekvenser av dette kan være at intervjuene blir kortere enn om en valgte å gjennomføre disse ansikt-til-ansikt. Svarene kan også bli mer konkrete og strukturen på intervjuet kan bli mer slavisk knyttet mot intervjuguiden (ibid.). I retrospekt kan en se at noen av problemene poengtert av Tjora (2012) var gjeldende i datainnsamlingen. Ved enkelte tilfeller falt samtaleaspektet bort og dybdeintervjuet ble i tilfellet tett knyttet mot intervjuguiden. I disse tilfellene ble intervjuene gjerne kortere enn ved tilfellene hvor samtaleaspektet var tilstedeværende.

Alle intervjuene ble tatt opp med samtykke fra informantene, opptakene ble gjort via mikrofon på datamaskin. Samtidig tok intervjuer fortløpende stikkordsmessige notater under intervjuet både for datagenerering men også for å generer nye oppfølgingsspørsmål knyttet til ytringer som var av interesse. Opptaket ble transkribert kort tid etter intervjuet var gjennomført. Intervjuer anså dette som mest hensiktsmessig da informasjonen satt ferskt i minne og en enklere kunne trekke linjer til de ulike forskningsspørsmålene. Etter intervjuene ble transkribert ble de sendt til de respektive informantene pr. mail for verifisering og at de kunne forsikre seg at de ikke var feilsitert.

4.3.4 Utvalg av informanter

Informantutvalget ble utarbeidet i samarbeid med veileder fra Bits AS, fokuset var å nå ut til informanter som besitter spisskunnskap knyttet til betalingsformidling. Deres kunnskapsgrunnlag vil gjøre dem i stand til å reflektere og formidle kunnskap om betalingsformidling som tjener oppgavenes problemstilling. En slik tilnærming til rekruttering av informanter betegnes av Tjora (2012, s. 145) som et strategisk utvalg. Utvalget av informanter er spredt mellom ulike organisasjoner som inngår i systemet for betalingsformidling. Informantutvalget var ønsket å belyse:

- NICS
- Open banking
- PSD2 og andre regulatoriske forhold
- Sikkerhetsarbeid i organisasjonen
- Sårbarheter i betalingsformidlingen

Den brede tilnærmingen virker hensiktsmessig i et systemet som preges av et flerfoldig aktørbilde med både banker, it-selskaper, fintech-aktører og myndigheter. For å fange kompleksiteten ble det derfor bestemt at informantutvalget skulle spenne bredt.

Tabell 4, informantutvalg

Informantutvalg	**Rolle i norsk betalingsformidling**
Informant 11	Fagrådgiver i større norsk bank.
Informant 21 Informant 22	Prosjektleder hos IT-leverandør av betydning for betalingsformidling. Produktadministrator hos IT-leverandør av betydning for Felles operativ infrastruktur.
Informant 31	CEO og co-founder hos fintechaktør
Informant 41	Seksjonsleder i sentralmyndighetene

En fordel knyttet til dette var hensiktsmessig inkorporering av perspektivene som de ulike aktørene besitter. En ulempe er at informasjonsgrunnlaget knyttet til hver informant ikke nødvendigvis reflekterer faktiske forhold, da dette er knyttet til deres personlige oppfatninger. På en annen side kan utvalget forsvares med at informantene besitter spisskunnskap knyttet til

betalingsformidlingen, dets sårbarheter, open banking, PSD2 og de nåværende trendene i betalingsformidling og –infrastruktur. Det kunne videre vært hensiktsmessig å inkludere informanter fra bigtech-aktører og internasjonale myndigheter som EBA.

4.3.4 Anonymitet og opptak

Informantene som deltok er blitt anonymisert og opplysninger knyttet til dem brukes ikke i studien. Fokuset for studien ligger på hvordan endringene i aktørbildet kan prege sikkerheten i betalingsformidlingen, derfor er informantenes kunnskap og synspunkt sentralt og ikke deres personlige egenskaper. Under alle intervjuene ble det gjort opptak med samtykke fra deltakerne. Dette var noe som ble forespurt i forkant av intervjudagen og før intervjuet. Opptakene ble benyttet til transkribering for enklere å analysere datamaterialet. Opptakene ble etter transkribering sendt til informantene for godkjenning, av fem informanter er det kun én som har ønsket endringer eller følt seg feilsitert. En tidsperiode etter transkriberingen var sendt til informantene ble opptakene slettet, uavhengig av om informantene hadde respondert på transkribert intervju eller ei.

Informantene er kategorisert i henhold til deres rolle i betalingsformidling, de identifiseres i fremstillingen av empiri ved bruk av tallkoding. Informantene er skilt ved deres rolle i betalingsformidlingen i Norge, inndelingen skiller mellom: banker; it-selskap/datasentraler; fintech-selskap og myndigheter. Det første sifferet skiller informantene i henhold til hvilken kategori de faller innenfor, det siste sifferet skiller informantene. Informanter tilknyttet banker begynner med nummerering fra 11-19, informanter knyttet til it-selskap har fått nummerering 21-29, fintech-selskap 31-39 og informanter knyttet til myndigheter har nummerering 41-49.

4.4 Validitet, reliabilitet og etiske utfordringer

4.4.1 Validitet

Tjora (2012, s. 206) betegner validitet som om en svarer på spørsmålene som stilles. Kvale (1997, i Tjora, 2013, s. 206) peker på at det finnes to former for validitet, kommunikativ og pragmatisk validitet. Den kommunikative validiteten finner en i dialog med andre forskere, ergo ved konferanser og eller publisering i vitenskapelige skrifter. Den pragmatiske validiteten stiller spørsmål ved hvorvidt forskningen som er gjort fører til endring eller bedring. Validiteten styrkes ved sterk reliabilitet og refleksivitet knyttet til valg av metodikk og teori. Den mest sentrale kilden til høy validitet er at den er tett forankret innen fagdisiplinen og gjerne tidligere forskning (Tjora, 2012, s. 207). Forankringen skal bidra til at spørsmålet en stiller blir svart på. Studien belager seg på kjente teoretiske bidrag som er godt

anvendelige for ulike system. Prinsippene for arbeid med samfunnssikkerhet er generisk utviklet og i så måte også anvendelige til problemstillingen. På bakgrunn av dette, vurderes validiteten til å være tilstrekkelig. Samtidig er det gjennom en vurdering knyttet til valg av metodisk tilnærming også vist til refleksivitet og svakheter ved studiens metodikk.

Samtidig kan manglende teoretisk analyse svekke validiteten da forskningsspørsmål 1 og 2 ikke blir belyst av teori. En kan derimot argumentere med at forskningsspørsmålenes formulering medførte noe behov for en slik analyse. Videre kan det også poengteres at i forskningsspørsmål 3 innlemmes empirien benyttet i FS1 og FS2 til å analysere konsekvensene av nye aktører i betalingsformidlingen. Det kan derfor argumenteres for at studien knyttes opp mot eksisterende teori innen fagdisiplinen samfunnssikkerhet. Et ytterligere aspekt som svekker validiteten er hemmelighold rundt fysiske og logiske sikringer i betalingsformidling. Av naturlig årsaker foreligger det hemmelighold rundt dette, men dette er fortsatt noe som svekker validiteten da studien ikke nødvendigvis i tilstrekkelig grad besvarer studiens problemstilling og tilhørende forskningsspørsmål.

4.4.2 Reliabilitet

Reliabilitet omhandler ifølge Ringdal (2013, s. 96) påliteligheten ved målingene som foretas, mer spesifikt om samme måleinstrument utvikler det samme resultatet ved flere målinger. Et slikt parameter er hensiktsmessig for å vurdere kvantitative, men ikke kvalitative studier (Thagaard, 2018, s. 188). I kvalitative studier må en isteden ifølge Thagaard (2018, s. 188) argumentere for studiens reliabilitet. En må derfor redegjøre for utvikling, fremgangsmåte og generering av primærdata. Argumentasjonen burde overbevise leseren om at dataen produsert er av kvalitet, ergo vil logikk tilsi at det samme gjelder for resultatene. Beskrivelsen av forskningsprosessen bør være konkret og transparent, reliabiliteten blir så økt ved at leseren kan lese og vurdere vitenskapelig ståsted, metodologi, forskningsprosessen, datainnsamling og utvalgsstrategi (ibid.).

Videre er det hensiktsmessig å vurdere hvordan informantenes subjektivitet har preget deres respons og tanker knyttet til endringer i betalingsformidlingen. Av naturlige årsaker kan en vente at svarene vil farges av informantenes rolle, alder og kunnskap i og om betalingsformidlingen. Dette er et forhold som kan innvirke på reliabiliteten til studien, da en ikke kan måle hvorvidt informantenes syn vil være oppfattes likt ved gjentatte målinger. Videre er det poengtert at forskerens subjektiviteten vil kunne prege analysen av datagrunnlaget. Forskeren kan i tilfeller også ha et forutinntatt syn på hvordan et system fungerer, noe som kan føre forskerens analyse for å støtte oppunder det opprinnelige synet. I

forbindelse med studien kan det argumenteres for at forskeren ikke har hatt inngående kunnskap om feltet på forhånd, ergo vil en forutinntatt vurdering være vanskelig å oppnå.

Reliabiliteten til studien kan vurderes å være noe god, primært fordi forskningsprosess, datainnsamling og utvalgsstrategi er redegjort for. Videre ligger intervjuguidene som er benyttet vedlagt, dette styrker reliabiliteten ytterligere ettersom leseren kan lese detaljert hvordan primærdataen er innhentet. Referanselisten og referanseføring er også noe som indikerer god reliabilitet, dette gjør det mulig for leseren å se hvor teorier og empiri er hentet fra. Reliabiliteten kan dog svekkes noe ved at transkriberingen av intervjuene ikke er vedlagt, årsaken til dette er grunnet plassmangel og informantenes anonymitet.

4.4.3 Etiske utfordringer

Tjora (2012, s. 199) poengterer at er det hensiktsmessig å anonymisere informantene i kvalitativ forskning, særlig i forbindelse med om det håndteres følsomme temaer. Selv om dette ikke er tilfellet ved denne studien er det valgt å anonymisere informantene. Årsaken til at dette er gjort er både grunnet personvern knyttet til informantene og deres stilling at deres person ikke er sentral for analysen. For å forsikre informantene om anonymisering ble det transkriberte intervjuet oversendt og de hadde dermed muligheten for å rette opp feil og si ifra om det var ting de ville ha unnlatt fra studien.

Det har gjennom studien vært fokus på å ivareta informantenes anonymitet, årsaken til dette er hovedsakelig at betalingsformidling ikke er et stort felt med mange deltakere. Personer innen feltet er gjerne kjent på tvers av organisasjoner og foretak, personvernet til informantene er derfor viktig å bevare. Det oppfattes som at informantenes personvern er godt ivaretatt gjennom studien.

4.5 Fordeler og ulemper ved metode

Bruk av kvalitativ metode har vært hensiktsmessig for å belyse problemstillingen. Metoden har midlertidig ikke kun hatt fordeler ved seg. Metoden viste seg ressurstung da en først måtte avdekke hvilke informanter som var aktuelle å prate med, videre måtte informantene kontaktes og det måtte settes en dato for intervju. Flere av informantene er i sentrale stillinger og har derfor begrenset tid, derfor har det ved flere tilfeller vært flere forsøk på fastsettelse av dato for intervju. Ressursbruken i forhold til kvantitativ metode, og dets omfang gjør at metoden ikke nødvendigvis vil ha samme evne til generalisering som ved en kvantitativ metode.

De semistrukturerte dybdeintervjuene presentere derimot ulike vinklinger, prioriteringer og syn på hva ansett som viktig. Samtidig var det forhold hvor informantene var enige. Semistrukturerte dybdeintervju presenterte også en arena hvor informantene kunne gå i dybden og utbrodere omkring hvordan trendene i betalingsformidling innvirker på deres oppgaver. Samtidig medførte denne fleksibiliteten at intervjuene hadde ulik lengde, avhengig av informant. Enkelte tilfeller ble det stadig presentert ny informasjon hvor oppfølgingsspørsmål ble naturlig, i andre tilfeller ble intervjuguiden mer ledende. I etterkant kan en se både fordeler og ulemper ved at intervjuguiden var tilpasset de enkelte aktørene. Fordelene ved dette var hovedsakelig at informantenes spisskunnskap i større grad ble utnyttet, samtidig var det enkelte spørsmål i intervjuguidene som var like og dette ga ikke like gode svar hos alle informantene. En ulempe ved tilpassede intervjuguider var at en kanskje ikke fikk fanget opp et koherent bilde på hvordan aktørene ser betalingsformidlingen. Tilgjengeligheten til informasjon knyttet til sårbarhet i betalingsformidlingen var noe som av åpenbare grunner ikke var tilgjengelig. En konsekvens av dette var endringer i forskningsspørsmålene og et litt mer overordnet syn på betalingsformidlingen.

I retrospekt kan en også vurdere hvorvidt metodetriangulering kunne vært hensiktsmessig, hvor i tillegg til informanter med spisskompetanse kunne ved bruk av et kvantitativt utformet spørreskjema avdekke kulturelle trekk, sikkerhetsarbeid og trussel oppfatning i organisasjoner knyttet til betalingssystemet i Norge. En videre avgrensning av problemstilling og tilhørende forskningsspørsmål kunne også i retrospekt vært gjort. Problemstilling og forskningsspørsmål i denne studien har favnet bredt og ergo inkludert en rekke moment i norsk betalingsformidling. Det største problemet knyttet til dette har vært omfanget på studien, som er meget omfattende. Samtidig har det vært en omfattende prosess på å redusere omfanget. Herunder har det vært behov for vanskelige vurderinger om å utelate deler knyttet til betalingsformidlingen. Deriblant er ikke VPO eller CLS inkludert i oppgaven selv om disse er sentrale i NBO. Videre kunne meldingsformatene NIBE, BOLS, SWIFT og ISO 20022 bli ytterligere utbrodert for videre hensiktsmessig vurdering av sårbarheten i betalingsformidlingen. Det samme gjelder for den historiske utviklingen av norsk betalingsformidling som gi en god innsikt i dagens systemer. Dette ligger vedlagt i vedlegg 6 for leser som ønsker å fordype seg. Grunnet studiens omfang har mye tid gått med på å redusere omfanget, noe som har vært problematisk med tanke på tid.

5. Empiriske funn

Kapittelet presenter de ulike funnene, som benyttes for å avdekke problemstillingen. En kan da innlede med problemstillingen for å gi en klarere kontekst.

> *Hvilke potensielle konsekvenser kan introduksjon av nye aktører i betalingsformidlingen ha for samfunnssikkerheten?*

Presentasjonen av empiriske funn forsøker å besvare problemstillingen gjennom å belyse forskningsspørsmål 1 og 2. Forskningsspørsmål 3 drøftes i kapittel 6. Kapittel 5.1 omhandler forskningsspørsmål 1, og kapittel 5.2 er dedikert til forskningsspørsmål 2. Fremleggelsen av empiri skiller ikke mellom dataen som er innhentet, primær- og sekundærdata brukes her om hverandre.

5.1 Verdikjedens utsatthet

Det er hensiktsmessig å presentere forskningsspørsmålet for å gi kontekst til funnene. Forskningsspørsmål 1 tar for seg hvordan nye aktører tar del i verdikjeden.

Hvordan introduseres nye aktører inn i norsk betalingsformidling?

For å hensiktsmessig besvarelse spørsmålet inkluderer trendene som preger betalingsformidlingen og en beskrivelse av aktørene som introduseres. Kapittelet begynner med førstnevnte og dernest går videre i å beskrive hvilke gjennom mekanismer nye aktører kan introduseres til den norsk betalingsformidlingen. Avslutningsvis vies det plass til en vurdering angående et potensielt fremtidig aktørbilde i betalingsformidling.

5.1.1 Trender i betalingsformidlingen

Digitalisering har åpnet for at bankene og betalingsforetakene har kunne tilby nye brukertjenester. De nye betalingstjenester, samt digitaliseringsprosessen i den norske betalingsformidlingen er en av grunnene til hvorfor tjenestetilbudet i Norge oppleves å være godt. Parallelt med utviklingen i Norge hvor bankene, datasentraler, underleverandører og myndigheter i fellesskap har utviklet betalingsformidlingen (Haare & Solheim, 2011), har digitaliseringen åpnet opp for nye aktører og nisjer. Nå forventes det at nye aktører vil gjennom ulike kanaler vil ta en del i aktørbildet i norsk betalingsformidling. Det er hovedsakelig identifisert tre kanaler med egen- og fellestrekk som nye aktører kan introduseres og inkluderes gjennom.

Reguleringer

PSD2, det nye EU-direktivet, åpner for deling av kontoinformasjon fra banker og ut til tredjepartstilbydere av betalingstjenester. Direktivet er ventet å fungere som en katalysator for nye betalingstjenester og tilbydere. En kan da forvente at nye aktører ønsker seg inn i bankenes verdikjede for betalingsformidling (Finanstilsynet, 2017a, s. 11). Særlig to ting ved direktivet har innvirkning for bankene, de må tilgjengeliggjøre betalingstjenester og kontoinformasjon til tredjepartstilbydere. Det kreves at bankene må åpne ene sine IT-løsninger, slik at tredjeparttilbydere av tjenester får tilgang til informasjon om bankkundene og kan gjennomføre betalingstjenester basert på kundene sine bankkontoer (Norges Bank, 2018a, s. 12). Direktivet bygger på en ny forretningsstruktur som kalles *open banking*, hvor informasjon deles gjennom dedikerte grensesnitt til tredjepartsaktører. På dette viset kan tredjeparter tilby tjenester til markedet (Brodsky & Oakes, 2017, s. 2). Open banking er noe som kan utfordre og samtidig hjelpe bankene i utvikling av betalingstjenester. Forretningsstrukturen vil sammen med PSD2, legge til rette for et mye mer mangfoldig spekter av aktører. Samtidig foreligger det begrensninger på hva tredjepartsaktørene får tilgang på gjennom PSD2.

> *De vil ikke få tilgang til det samme som bankene, men de vil få tilgang til et standardisert grensesnitt på toppen av bankene, som de kan bruke til betalinger. (Informant 21).*

Forventningen om endringer nå som PSD2-direktivet er innført i Norge fra og med 1. april 2019 gjennom § 11 i Betalingssystemloven (1999) er noe dempet (Finanstilsynet, 2019, s. 6). Bankene er pålagt å tilgjengeliggjøre åpne grensesnitt innen 14. september 2019. Direktivet gir samtidig tredjepartsaktører som melder grensekryssende virksomhet tilgang til betalingskontoer i andre land, deriblant Norge (ibid. , s. 16-17).

Open banking

EU's reviderte betalingsdirektiv er følgelig en sentral bidragsyter til hvorfor vi på sikt kan vente å se endringer i landskapet for betalinger. Det er dog ikke den eneste måten nye aktører kan introduseres til betalingsformidling. Nye aktører kan inngå i bi- eller multilaterale open banking-samarbeid med banker. Som poengtert av Brodsky og Oakes (2017) er open banking er i større grad en plattform for informasjonsdeling fra bankene til tredjepartene (Brodsky & Oakes, 2017, s. 2).

> *Vi har sagt at tilgangen basert på PSD2 er regulert, mens tilgangen basert på open banking er ikke regulert og krever mye bedre avtale og sikring mellom aktørene og ikke minst i forhold til brukerne. Så hvis det er noe jeg skulle nevne så er akkurat den tematikken der. (Informant 41).*

I open banking så reguleres adgangen og tilgangen til informasjonen tredjepartsleverandører gjennom avtaleforhold knyttet til banken (Evry AS, 2017, s. 24). Skillet mellom tilgang via open banking samarbeid og tilgang gjennom PSD2 er tilgangen som gis tredjepartsaktørene. I open banking kan banken velge å benytte seg av lukkede grensesnitt som kun aktører de samarbeider med får tilgang til (ibid., s. 28).

> *Når det gjelder open banking er det egentlig et produkt og tjeneste bankene kan tilby til aktører de ønsker å samarbeide med. Da vil det være andre mekanismer som styrer tilgangen til de tjenestene, og hvor det vil være en avtale og et forhold hvor banken og den tredjepartsaktøren sender til hverandre. Og som får følger for tilgang, beredskap og tjenester (Informant 11).*

Flere av bankene har allerede tatt bruk av dette, i utviklingen av sitt tjenestetilbud. Open banking tillater utvikling av brukergrensesnitt hvor tjenester fra andre banker kan inkorporeres sammen for en mer gunstig brukeropplevelse (Finanstilsynet, 2019, s. 49). Inntoget av store aktører som Apple, Google, Garming og Fitbit skyldes i stor grad bankenes villighet til å dele informasjon knyttet til sine tjenester. Samarbeidet med bigtechaktørene er særlig knyttet opp mot kortbetalinger og at kunder nå har muligheten til å kunne betale gjennom løsningene presentert av aktørene. Dette omhandler særlig betaling knyttet til telefon og klokker (ibid., s. 15). Generelt for denne inngangen til betalingstjenester er at deltakende tredjepartsaktørene ikke nødvendigvis er underlagt reguleringer knyttet til deres tjenestetilbud, herunder blir det derfor en vurdering fra bankens side som defineres tredjepartens tilgang.

5.1.2 Outsourcing av bankenes oppgaver.

Outsourcing av tjenester og oppgaver er ikke et nytt fenomen, men noe som har vært tilstedeværende i forretningsaktiviteter siden 1980-tallet (Lonsdale & Cox, 2000, s. 47). Tjenesteutsettelse av aktiviteter har gjerne et rasjonale knyttet til beslutningen. Faktorer som ressurser, kompetanse, leveranse, kjerneaktiviteter og økonomi spiller inn i slike beslutninger (Gottschalk, 2013, s. 24-25). Outsourcing er dog ikke utenfor innvirkning fra tilsynsmyndigheten i Norge. Det foreligger det en hjemmel for Finanstilsynet i Finanstilsynsloven (1956) § 4 c. for å både motta opplysninger om utkontraktering av tjenester, samt pålegg om å stanse eller avslutte prosessen. I henhold til utkontraktering av sentrale tjenester spiller tilsynsmyndighetene en vesentlig rolle i å tilse at foretak i Norge ikke sender ut tjenester som kan innvirke på deres konsesjonsbelagte plikter. Det kan også foreligge andre lovpålegg eller forskrifter foretakene må vurdere ved outsourcing, slik at de og underleverandørene er i tråd med bestemmelsene (Finanstilsynet, 2019, s. 30).

Flere banker og næringen generelt outsourcer deler av sin verdikjede innenlands til kjente IT-bedrifter (NOU 2015:13, s. 175), men det offshores også utenlands (Finanstilsynet, 2017a, s. 34). Utover drift, foreligger det trender som indikerer at skytjenester er noe som benyttes mer flittig av foretakene (Finanstilsynet, 2019, s. 8). Skytjenester er av Datatilsynet (2018a) definert som en «samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internettet». Herunder skilles det mellom tre hovedformer for skytjenester: SaaS[17], PaaS[18] og Iaas[19].

> *..Fordelen for oss er det at hele produktporteføljen vår er bygget på en GoogleCloud-plattform og vi har bygget på en utviklingsprosess og metodikk som er ganske moderne, i mangel på et bedre ord. Og der er veldig mye sikkerhet ivaretatt, jeg tror banker, gamle tradisjonelle banker har mye større utfordring i å beskytte dataene sine fordi de er gamle, store komplekse systemer med utdatert teknologi. Mens vi får veldig mye gratis ved å bruke den nye teknologien. (Informant 31).*

Bruken av skyløsninger er tiltakende og nyere aktørene benytter seg av skytjenester som en sentral del knyttet til ens produktplattform. De største aktørene innen denne type tjenester er bigtechaktører som blant annet Microsoft, Google og Amazon (Finanstilsynet, 2019, s. 32). Informanten ser at deres bruk av skytjenester er noe som gir foretaket en fordel og at dataen oppleves tilstrekkelig beskyttet i skytjenesten. I synet på foretakenes bruk av skytjenester skriver Finanstilsynet (2019, s. 31) at foretakene i stor grad gjør tilstrekkelige vurderinger knyttet til ulike risikoer og sårbarheter. Enkelte av virkene som settes ut krever samtidig kryptering og flerfaktorautentisering for å tilstrekkelig beskytte dataen liggende hos tjenesten (ibid.).

5.1.3 Potensielt fremtidig aktørbilde

I lys av de dyptgående endringene som preger og innvirker i bankenes økosystem for betalinger, kan en vente å se endringer i aktørbildet med tilbydere av betalingstjenester. En slik endring er dog ventet å være noe moderat, særlig i et kortsiktig perspektiv. Samtidig kan man allerede nå identifisere ulike grupper av aktører som fremtidig kan ha innvirkning på betalingsformidlingen i Norge.

Fintechs

Begrepet fintech er definert veldig løst og fungerer i dag som et samlebegrep for ny finansiell teknologi og nye aktører (Finansdepartementet, 2018a, s. 35). Nye teknologiske vinninger

[17] Software as a service/programvare som tjeneste.
[18] Platform as a service/plattform som tjeneste.
[19] Infrastructure as a service/infrastruktur som tjeneste.

som blockchain, biometri, digital valuta er noen av disse nye nyvinningene utvikles og introduseres. Nye aktører forventes å ta nytte av ny teknologi i sin tjenesteytelser, både små og store bedrifter kan benytte teknologien som tredjepartstilbydere av informasjons- og betalingstjenester (ibid., s. 36). Implementeringen av nye løsninger åpner for effektivisering, inntjeningsmuligheter og økt brukervennlighet. Samtidig vil implementering av nye teknologiske løsninger og introduksjon av nye selskap kunne medføre risiko med tanke på betalingsløsninger (Finanstilsynet, 2017b, s. 21). I dag er Vipps den største og mest fremtredende fintechaktøren i Norge, dette er utviklet i samarbeid med bankene. Andre aktører som KLARNA og Payr gjør seg også bemerket med sine løsninger. En kan derimot se at en rekke aktører har startet opp.

> *..Det er vel 5500 fintechs-startups i Europa. Det er mange innenfor payments, mange innenfor b2b-technology licensing og konsulentselskapene til bankene, det er mye på lending, en del på marketplace, regtech, insuretech. Ja, det blir bare lister. For jeg vet nesten ikke hva jeg skal si, for det er ganske komplekst å få oversikt over det landskapet. (Informant 31).*

Som tidligere poengtert åpner PSD2 for internasjonal konkurranse for betalingstjenester (Finansdepartementet, 2018a, s. 59; Knudsen, 2019). Pågangen av nye aktører er dog ventet til å være noe moderat i nærmeste overskuelige fremtid (Finanstilsynet, 2019, s. 16). Flere informanter poengterer at den strenge reguleringen som omgir direktivet kan hemme en hurtig fremvekst av tilbydere.

> *Det PSD2 var skrevet og ment for å gjøre var å lage et sikrere system men samtidig å åpne for konkurranse ved å fjerne en del av de barrierene som bankene har bygget rundt sine tjenester. For å gi bedre tjenester og vilkår til brukerne, det var det PSD2 i utgangspunktet var ment til å være. Det det nå har blitt gjennom intens lobbyering fra de mer etablerte aktørene, er en veldig strupet og begrenset effekt. (Informant 31).*

Informant 31 beskrivelse av direktivet presenterer et noe unikt perspektiv på reguleringen, da vedkommende er direkte påvirket av reguleringen. Informantens syn samsvarer med hva Finanstilsynet (2019, s. 16) beskriver som hva de forventer som en «*moderat pågang av konsesjonssøknader fra nye aktører*». Det er forventet at de som vil tjene mest på dette, særlig på kort sikt, er bankene som kan velge å benytte seg av hverandres PSD2-grensesnitt. På denne måten kan bankene tilby tjenester hvor deres kunder kan ha fullstendig oversikt over sine betalinger knyttet til forskjellige konti i ulike banker. Nye tredjepartsaktører må derimot imøtekomme en rekke krav og reguleringer knyttet til sikkerhet i sine tjenester, dette er noe bankene unngår ettersom de allerede har konsesjon for formidling av betalingstjenester.

Konsesjonen er noe nye aktører må få for å kunne tilby tjenestene PISP[20] og AISP[21] (ibid.). Direktivet åpner både for mindre aktører som fintechs, men det meldes allerede om flere bigtechaktører som har meldt sin virksomhet til Norge. Dette er dog i all hovedsak knyttet til bilaterale samarbeid med bankene (ibid., s. 17). Ikke-regulert open banking-samarbeid er samtidig en alternativ vei for aktører å tilby tjenester knyttet til betalinger eller kontoinformasjon med mer.

> *Vi har inngått flere bilaterale avtaler med de aller største bankene, men selv om avtalene er inngått så har de ikke åpnet opp APIene sine enda. Slik at det har ikke hatt noen effekt fordi vi har ikke, til syvende og sist, ikke kunne vise kontotransaksjonene til kundene våre i appen for eksempel. Vi har kun tilgang til test-APIen og sånne ting. Så er jo egentlig fortsatt ingen i Norge som har noe nasjonalt dekkende open banking tilbud. (Informant 31).*

Grensesnittene utviklet av bankene er pr. våren 2019 fortsatt ikke ferdigstilt i sin helhet, noe som er ventet å hemme nye aktører. Begrensninger til grensesnitt å benytte seg av legges til grunn for at inntoget av fintechs ventes å være begrenset, særlig i kort fremtid.

På lengre sikt kan en derimot kunne forvente, grunnet både at grensesnittene knyttet til PSD2 og andre proprietære grensesnitt vil være ferdigstilt, et bredere aktørbilde. Plattformen som da åpnes, presenterer muligheter for at nisjeaktører kan delta, samarbeide og utvikle funksjoner knyttet til betalingstjenester. Grunnet det manglende inntjeningspotensialet for aktører som ønsker å initiere betalinger, i PSD2 begrunnet i lovmessig hjemmel (PSD2, 2015, artikkel 62). En vil derfor ikke forvente at nye aktører gjennom enten PSD2-grensesnittene eller proprietære grensesnitt vil belage sin inntjening alene rundt ytelse av betalingstjenester. Direktivet åpner også for at nye aktører innen betalingsformidling i EU/EØS kan supplere aktivitetene med andre tjenester (PSD2, 2015, Artikkel 18). Det forventes at nye aktører som introduseres i betalingsformidlingen vil benytte seg av grensesnittene som åpnes til å tilby flerfoldige tjenester som vil gå utover selve det å gjennomføre betalinger initiert av brukeren.

> *Altså i utgangspunktet så skal ikke vi tjene penger på betalingsformidlingen (..) Så hele PSD2 og open banking og regningsbetalinger er egentlig bare en del av vår markedsføring, som en måte å få folk til å bruke tjenestene våre og så dekker vi alle de kostnadene. (Informant 31).*

I tråd med informant 31 kan nye aktører introdusere seg ovenfor brukere gjennom tilbud av betalingstjenester og på denne måten tiltrekke seg kunder. Norske fintechselskaper har eksempelvis spesialisert seg på regningsbetaling gjennom deres applikasjoner. Dernest bruker

[20] Payment Initiation Service Providers.
[21] Account Information Service Providers.

så transaksjonshistorie, regning- og kundeinformasjon for å tilby alternative leverandører til brukerne. Deres videre visjon er å bidra til optimalisering av økonomien til brukerne gjennom slike leverandørbytter. Sentralt for å kunne gjennomføre dette er nettopp PSD2 (Bakken, 2018).

Bigtech-selskaper

Aktørbildet i fremtiden vil i ytterligere grad potensielt preges av store teknologiselskap som allerede er tilstede i betalingsformidling. Google, Apple, Facebook, Amazon og lignende aktører kan ta en større del av finansielle tjenesteytelse i Norge og Europa generelt. Slike aktører har allerede en stor plattform med vesentlig brukerbase som de kan ta nytte av i tjenestetilbudet deres (Norges Bank, 2018a, s. 13).

> *Aktørene i betalingssystemet tilpasser seg teknologiutviklingen. Det har ført til endringer i både aktørbildet, konkurransesituasjonen og verdikjeden. Globale teknologiselskaper utvikler betalingsløsninger med utgangspunkt i sine store kundenettverk og eierskap til teknologiske plattformer. (Norges Bank, 2018a, s. 12).*

Det som skiller bigtechaktører fra fintechs er deres ressurser, kompetanse, store datamengder og at de allerede har et stort etablert nettverk til brukere (Langbraaten, 2012, s. 17; Norges Bank, 2018a, s. 4). De store teknologibedriftene som Apple, Facebook og Google har allerede utviklet løsninger som tillater sine brukere å benytte seg av sine betalingsløsninger og gjort sitt inntog i norsk betalingsformidling (Finanstilsynet, 2018, s. 15; Knudsen, 2019). Løsninger som Apple Pay, Google Wallet og P2P-betalinger og P2B-betalinger gjennom kanaler som Messenger og WhatsApp er allerede introdusert som fullverdige løsninger i USA. I Norge er betalingsapplikasjonene til bigtechselskapene dog kun pr. våren 2019 kun tilknyttet betalingskort (Norges Bank, 2019, s. 11).

Nets AS har for Nordea utviklet en chatbot som gjør det mulig initiere betalinger gjennom eFaktura via kommunikasjonsplattform Messenger (Nordea, 2017). Apple tilbyr løsningen Apple Pay til bruk i butikkterminaler samt betalinger over nett (Nordea, ingen dato). Google har også utviklet en løsning for mobilbetalinger, Google Pay, denne løsningen belager seg også på NFC-løsningen som Apple Pay benytter (Hopland, 2018). Garmin og Fitbit har også utviklet lignende løsninger som bruker NFC-teknologi, bare med smartklokker (Honningsvåg, 2018). Nærkontaktsløsningen NFC gjennom smarttelefon og klokker forutsetter en avtale med kortusteder som må ha en tjeneste som gjør det mulig og tokenisere kortinformasjonen til å lage en digital versjon av betalingskortet. Videre spekuleres det i om at Amazon ønsker seg inn i banknæringen (du Toit & Cheris, 2018).

Slike teknologiselskap besitter en stor brukerbase hvor de allerede sitter på store datamengder og kunnskap om sine brukere (Langbraaten, 2012, s. 17). Teknologifortrinnet som AI og Big Data, ansees dog av enkelte som ikke utfordrende ettersom bankene tidligere har og fortsatt driver ytterst kompliserte dataanalyser (Eide, 2017, s. 329-330). På en annen side kan disse bigtechselskapene i fremtiden operere som i mer eller mindre grad tradisjonelle banker gjennom datterselskap. Deres store kundesegment utgjør en virkelig trussel for de tradisjonelle bankene og deres næringsgrunnlag (Langbraaten, 2012, s. 17). En potensiell løsning for bigtechselskapene kan være bruk av e-penger og dermed operere som e-pengeforetak. Noen av bigtechaktørene har allerede etablert e-pengeforetak innen EØS (Finanstilsynet, 2017a, s. 12). Utviklingen vil kunne legge press på reguleringene som allerede foreligger er tilstrekkelige (Norges Bank, 2019, s. 4). Videre foreligger det spekuleringer at slike aktører ønsker å utvikle egne pengeenheter, slike pengeenheter som har betegnelsen stable coins vil forsøkes festes mot andre valutaer eller andre former for verdi. En slik valuta vil favnes ikke av eksiterende reguleringer og vil ved tilfellet ikke ha samme sikkerhet som eksisterende løsninger knyttet til e-pengeforetak og e-penger (ibid., s. 11).

Disse forventningene til tross, flere er heller pessimistiske i synet på innvirkningen potensielle nye aktører vil ha på inntjeningspotensialet til bankene. Eide (2017) illustrerer evnen organisasjoner har til å kunne tilpasse seg konkurranse ved inntoget til Über i Oslo, hvor lokale taxiselskap gjennomførte tiltak for å pleie kundeopplevelsen. Behovet for at bankene fatter lignende avgjørelser og tilpasser seg teknologien for å yte bedre kundeopplevelser ansees som kritisk (s. 331).

Underleverandører

Tendensen finansforetak har til å utkontraktere aktiviteter knyttet til sine tjenester er med på å introdusere nye aktører. De mest prominente aktørene i betalingsmarkedet er dog kjente i sammenheng med norsk betalingsformidling (NOU 2015:13, s. 170). Fortsatt foreligger det et behov for å outsource tjenester og aktiviteter blant norske foretak. Underleverandører inkluderer da norske og nordiske aktører, samt en økende tendens til å sette ut tjenester til utenlandske aktører. Offshoring av IKT-drift kan i så måte introdusere nye aktører til funksjoner og tjenester tilknyttet betalingsformidlingen. Flere har presentert mulige problemer, både for bedrift og myndigheter, i forhold til beredskapsløsninger, sårbarhetsvurderinger og risikostyring (Norges Bank, 2018a, s. 7). Uoversiktlige verdikjeder, sikkerhetskrav og omfanget av avtalen med eksterne leverandører er også noe som er problematisk med outsourcing av tjenester (Finanstilsynet, 2018, s. 21-22). Oversikt over

antallet underleverandører er forbundet med vanskeligheter, men en kan likevel forvente at tjenestene som outsources definerer underleverandørene. Et eksempel på dette er den prominente rollen få store IT-leverandører har for norsk betalingsformidling (NOU 2015:13, s. 170). Samtidig har den økende tendens foretak har til å outsource til skytjenester medført delvis inkludering av nye aktører i betalingsformidling, deriblant bigtechs som Google og Microsoft (Finanstilsynet, 2019, s. 32).

Oppsummering forskningsspørsmål 1

Tabell 5 Oppsummering funn FS1

Oppsummering funn FS1
- Norsk betalingsformidling kan forvente en moderat endringstakt i aktørbildet de nærmeste årene. - På lengre sikt kan en derimot forvente større endringer. - Nye aktører kan fatte kundens oppmerksomhet ved innovative og smarte løsninger for betaling, sparing og oversikt økonomien **PSD2** - PSD2 er sentralt for introduksjonen av nye tredjepartsaktører knyttet til betalingsformidlingen, gjennom åpne grensesnitt knyttet til bankene. - Grensesnittene er sterkt regulert som en følge av stort fokus på sikkerhet. - En venter derfor en moderat vekst i aktører introdusert via PSD2. **Open banking** - Open banking som forretningsplattform introduserer en alternativ kanal hvor tredjeparter kan gjennom dedikerte grensesnitt knytte seg opp mot bankene i bi- eller multilaterale samarbeid. - Ikke direkte omfattet regulering og krav som ved PSD2. **Outsourcing** - Outsourcing av tjenester presenterer en mulighet for underleverandører for å delta i verdikjeden for betalingsformidling. - En kjent strategisk begrunnet avgjørelse mange foretak benytter i utvikling og drift av tjenester og funksjoner. - Outsourcing av ens konsesjonsbelagte tjenester begrenses i stor grad av lovpålegg i norsk lov. - Er i stor grad tilknyttet drift og utvikling av tjenester og funksjoner. **Fremtidig aktørbilde** - Aktørbilde kan i nær fremtid forventes å være relativt likt som i dag, hovedsakelig grunnet de strenge kravene i PSD2. - En kan forvente at fintechs kommer inn i betalingsmarkedet med et produkt som omfatter mer enn kun betalinger. - På lengre kan bigtechs ventes å utvide sitt tjenesteutvalg og kan på sikt utfordre bankene, gitt førstnevntes ressurser, kompetanse og brukermasse. - Outsourcing begrenses ikke kun til innenlands aktører, offshoring introduserer internasjonale aktører. - Bruken av skytjenester er noe som øker i omfang. Herunder også tilstedeværelsen til større bigtech-selskap.

5.2 Forskningsspørsmål 2

Forskningsspørsmål 2 omhandler hvilken potensielle sårbarheter en kan forvente med inntoget av nye aktører.

Hvilke sårbarheter tilfører nye aktører i betalingsformidlingen?

Spørsmålet spør om hvilke sårbarheter en kan forvente at oppstår som en følge av endringer i aktørbilde i betalingsformidlingen. Engen et al. (2016, s. 47) og Renn (2008, s. 69) forståelse av begrepet som systemets forutsetning eller manglende evne til å fungere ved eller etter en hendelser, legges her til grunn. Samtidig må sårbarheter sees i lys av risiko, ens omgivelser, og endringer (Renn, 2008, s. 62). I forsøk på å besvare forskningsspørsmålet blir det da hensiktsmessig å presentere hvilke sårbarheter som allerede er identifisert; trusselbildet som preger betalingsformidlingen; og hvordan det jobbes med sikkerhet og beredskap før en kan vurdere hvilke potensielle sårbarheter som kan oppstå i betalingsformidlingen. Kapittelet presenterer innledningsvis sårbarheter, beredskapsløsninger og sikkerhetsarbeidet som foreligger i norsk betalingsformidling. Avslutningsvis vurderes hvilke potensielle sårbarheter som kan oppstå i norsk betalingsformidling.

5.2.1 Hvilke sårbarheter eksisterer i norsk betalingsformidling?

5.2.1.1 Felles operativ infrastruktur

Sentralt i norsk betalingsformidling er den felles operative infrastrukturen, dette er kjernen i det selvregulerte betalingssystemet. Herunder vil bortfall av tjenester levert av FOIene kunne medføre vesentlige problemer for leveranse av betalingstjenester til det norske samfunnet (Finanstilsynet, 2018, s. 29; NOU 2015:13, s. 175). For å gjennomføre en betaling må alle ledd som inngår i transaksjonen fungere. Sårbarheter og konsekvenser i FOI kan sees i asymmetrisk symbiose. Sårbarheten og sannsynligheten for feil er størst i leddet hvor transaksjonene initieres, men konsekvensene ved avvik stiger jo lengre opp i verdikjeden en kommer (NOU 2015:13, s. 174). Funksjonaliteten i den norske betalingsformidlingen er i vesentlig grad bygget opp rundt felles løsninger og samordning (ibid., s. 168). FOIene er derfor ytterst sentrale for norsk betalingsformidlings funksjonalitet.

> *BankID, BankAxept og NICS er en del av felles operasjonell infrastruktur for bankene. For øvrig er bankenes IT-drift spredd på flere driftsmiljøer og/eller -steder. Dersom en hendelse ikke rammer felles operasjonell infrastruktur, er det lite sannsynlig at mer enn ca. 40 prosent av bankkundene samtidig kan rammes av en hendelse. (Finanstilsynet, 2018, s. 29).*

Bortfall av FOIene i betalingsformidlingen vil ha vesentlige konsekvenser for leveransen av en trygg og sikker betalingsformidling. Sårbarheter knyttet til FOI vil derfor kunne ha store ringvirkninger for muligheten en har til å initiere og gjennomføre en betaling.

Interbanksystemet

For å kunne generere interbanktransaksjoner må bankene være tilknyttet Bits AS gjennom medlemskap i Finans Norge, eller særskilt tillatelse fra Bits AS eller Norges Bank (Bits AS, 2018c, s. 2). Transaksjoner som favner innunder det norske betalingssystemet, herunder via FOIene, felles betalingstjenester og eller påvirker bankens posisjon i NBO skal gjøres gjennom avregningssystemet NICS. Konsesjonen for drift av systemet er underlagt Bits AS, Bits AS er ansvarlig for at NICS driftes i henhold til Betalingssystemloven (1999) og krav fra Norges Bank (Bits AS, 2018a, s. 4). Den tekniske driften av avregningssystemet er satt ut til NNI[22] (ibid., s. 10).

Utkontrakteringen av den tekniske driften er tilknyttet en operasjonell risiko ved at avregningssystemet for transaksjoner er satt ut til én aktør, NNI. NNI er et datterselskap av Nets, som er en stor IT-aktør som yter tjenester til bankene. Dette kan konstruere en konsentrasjonsrisiko da flere tjenester av betydning er knyttet til to selskap i nær relasjon (Finansdepartementet, 2018a, s. 88). Samtidig er det etablert to driftssteder for NICS som er innen geografisk hensiktsmessig avstand, dette er noe som skaper redundans i løsningen dersom et driftssted faller ned (Norges Bank, 2018a, s. 28). Et av driftsstedene er dog lokalisert på samme plass som andre aktører sentrale for den finansielle stabiliteten i Norge (ibid.). Dette er igjen noe som gjennom økt konsentrasjonsrisiko kan ha en innvirkning på sårbarheten. Norges Bank (2018a, s. 24) har vurdert den operasjonelle risikoen til NICS i henhold til prinsipp nedsatt av CPMI-IOSCO[23]. Generelt vurderes risikoen til å være godt håndtert, med et unntak som er mangler knyttet til beredskapsløsningene. Mangler knyttet til beredskapsløsningene er noe en kan betegne som sårbarheter i systemet. Videre presiseres det at ny vurdering vil finne plass, for å vurdere en av driftslokasjonene til NICS (ibid.). I vedlegg 6 *Tiltak ved omfattende avvik i betalingsinfrastrukturen* til *Regler for avregning og oppgjør av transaksjoner* presenterer Bits AS (2018f) ulike tiltak som kan fattes ved større avvik i funksjoner knyttet til eller direkte i NICS. Et av tiltakene presenterer at det foreligger alternative løsninger for innsending og mottakelse av transaksjoner i NICS (Bits AS, 2018f, s. 1). Det indikeres at systemet i stor grad er å anse som robust. Et større avvik i 2018 knyttet til

[22] Nets Norge Infrastruktur.
[23] Committee on Payments and Market Infrastructures-International Organization of Securities Commissions.

NICS stoppet likevel opp avregningen i flere timer, noe som forsinket betalingsformidlingen i flere timer (Bits AS, 2018a, s. 3). Noe som peker på tidssensitiviteten i systemet.

Deltakelse i interbanksystemet er begrenset av Betalingssystemloven (1999, kapittel 5), samt deltakelse i NICS er underlagt vurderinger fattet hos Bits AS (Bits AS, 2018c, s. 2). Dette aspektet er noe en kan vurdere som et risikoreduserende. Adgangsregulering kan forhindre at aktører som ikke etterlever tilstrekkelig sikkerhetskrav deltar i bankavregningen. Deltakerne i avregningssystemet må også, i regi av Bits AS, gjennomføre selvsertifisering og egenvurdering annethvert år (Bits AS, 2018a, s. 9-10). Nivå 1-banker må gjennom en selvsertifisering som er noe mer omfattende, mens nivå 2 bankene må foreta en egenevaluering (ibid.). Ordningen er ment for at bankene selv skal vurdere sine beredskapsrutiner og kommunikasjonskanaler ved avvik knyttet til NICS. Dette ansees som en risikoreduserende aktivitet. Det oppleves fra Bits AS at ordningen er noe bankene tar seriøst. Alle nye aktører som vil tilknyttes NICS må gjennomgå selvsertifisering eller selvevaluering i forkant av deltakelse (ibid., s. 21). Aktiviteten er av informant 22 ansett som særs hensiktsmessig.

> *Det er jo en av grunnprinsippene for hele betalingssystemet, at det skal være selvregulert. Da er det bankene som har ansvaret for egen sikkerhet, oppfølging av dataleverandører også. Så jeg synes det er et viktig prinsipp og jeg håper det er tilstrekkelig ja. Det gjør at det ikke blir detaljstyring, det kan jo ha negative konsekvenser om et sentralt organ skal sitte å styre hvordan ting skal gjøres. Vi har et veldig bra mangfold i Norge, risikoen er spredt over mange deltakere. Så selvevaluering og egenvurdering det er et viktig prinsipp, synes jeg. (Informant 22).*

Som av kapittel 2.2.1 presenteres bankenes økosystem for betalinger som i stor grad selvregulert. Ansvaret knyttet til generell sikkerhet og spesifikk betalingssikkerhet i stor grad lagt hos deltakerne selv. Aktiviteten med selvsertifisering og selvevaluering er et aspekt ved banknæringen som kan gjøre den mer observant omkring deres egne sårbarheter, rutiner, samt at det bidrar til opplæring og bevissthet hos bankene (Bits AS, 2018a, s. 21).

Ved interbanktransaksjoner foreligger det i tillegg til kapital også informasjon som skal gi informasjon knyttet til transaksjonen. Meldingsutvekslingen kan gjøres gjennom meldingsformatene NIBE, BOLS, SWIFT og ISO 20022.

> *NIBE er vel egentlig ganske bra uten at vi skal gå noe mer inn på det. BOLS er vel litt begrenset og vi også håper jo at man skal gå over til nye standarder som er enklere og mer fremtidsrettet. Og vi gjør det vi kan, vi kommer med våre argumenter. (Informant 22).*

Sitatet viser informant 22 sitt syn på standardene NIBE og BOLS. Av meldingsstandardene er BOLS den eldste og omfatter i dag primært korttransaksjoner og dekningskontroll (Bits AS, ingen dato(e)). NIBE er noe nyere og er basert på EDIFACT-standarden (Bits AS, ingen dato(c)). Det begrensede bruksområdet til BOLS kan være en konsekvens av dets levetid og at den er en proprietær standard (Bits AS, ingen dato(e)). Videre er det en svakhet med både BOLS og NIBE at standardene ikke er krypterte, det er dog påbegynt arbeid som sikter på også gjøre disse meldingsformatene kryptert (Bits AS, 2018a, s. 12). I transaksjonsløypen i NICS går alle BOLS-transaksjoner til en av de fem daglige nettoavregningene. NIBE-transaksjoner hvor beløpet er over 25 millioner går til bruttoavregning, øvrige NIBE-transaksjoner går til nettoavregning (Bits AS, 2018e, s. 1).

SWIFT er et internasjonal kooperativ, eid av dets medlemmer. Gjennom medlemskap i SWIFT har medlemmene tilgang til et standardisert meldingsformat som kan benyttes til transaksjoner globalt og lokalt (SWIFT, ingen dato.). I Norge benyttes SWIFT både til netto- og brutto avregning. Bruttomeldinger med SWIFT kan sendes dersom transaksjonen er merket REG eller HASTE eller om transaksjonsbeløpet overskrider 25 millioner. Øvrige SWIFT-transaksjoner inngår i nettoavregningen (Bits AS, 2018e, s. 1). Alle SWIFT-transaksjoner er krypterte (Bits AS, 2018a, s. 12), noe som gjør det vesentlig mindre sårbart ovenfor målrettede angrep.

Internasjonale trender og oppslutning rundt meldingsstandarden ISO 20022 har medført at de nasjonale proprietære standardene vil utfases for ISO 20022 (Bits AS, ingen dato(f)). Meldingsformatet har en fordel da det erstatter eksisterende standarder og samtidig kan øke funksjonaliteten til meldingsstandardene (Bits AS, 2016a, s. 7). Samtidig er standarden beregnet på hele verdikjeden for betaling, fra initiering til mottak av betalinger (Bits AS, ingen dato(f)). På bakgrunn av dette, samt internasjonale trender er det ventet en overførsel til denne meldingsstandarden. En kan derfor forvente en gevinst ved forenkling av prosessene som involverer, bedre løsninger for aktørene og lavere kostnader knyttet til bruk av formatet (Bits AS, 2016b, s. 10).

Andre FOIer

BankAxept er ikke utelukkende en kortscheme, det er også en sentral del av den felles operative infrastrukturen i norske betalingsformidling. Noe av viktigheten til BankAxept kan tillegges at dette er den fremste kortløsningen i Norge (Norges Bank, 2018a, s. 13; NOU 2015:13, s. 175). BankAxept blir derfor sentralt for gjennomføring av kortbetalinger i norsk

betalingsformidling. Bortfall av tjenesten vil derfor ha store ringvirkninger for evnen brukerne har til å gjennomføre betalinger (NOU 2015:13, s. 175).

Angående hva som er mest kritisk, så ville jeg kanskje sagt at betalingssystemer i varehandelen er det som ville gjort umiddelbart utslag og oppfattet som kritisk for samfunnet. (Informant 11).

Løsningen knyttet til BankAxept driftes av NNI, det foreligger krav til driftsoperatøren om tilstrekkelige beredskapsløsninger for drift av tjenesten (Finans Norge, 2017, vedlegg 2). Beredskapen for drift av systemet ivaretas av at det er etablert to geografiske avgrensede driftslokasjoner med ulike leverandører av kommunikasjon. Om driftslokasjonene begge skulle være nede vil en fortsatt kunne gjennomføre handel gjennom en reserveløsning (ibid.).

Det er jo sånn i dag at norske kunder har tilgang på flere forskjellige betalingsnettverk både BankAxept, Visa og MasterCard. Dersom BankAxept som betalingssystem faller ned, så vil en fremdeles kunne bruke betalings Visa- og MasterCard-delen av betalingskortene de aller fleste steder. (Informant 11).

Visa- og MasterCard-løsningene er også alternativ som skaper redundans i kortbetalingsløsningene. Disse kan figurere som alternative innsamlere og transaksjonsløyper i de tilfeller BankAxept-løsningen opplever nedetid. Det må dog bemerkes at Visa og MasterCard ikke er reserveløsningene for bortfall av kommunikasjon. Ved bortfall av kommunikasjon vil tjenestene på lik linje med BankAxept ikke kunne fungere tilstrekkelig. Reserveløsningen er knyttet til betalingsterminalen satt ut på brukerstedet og vil kunne være funksjonell så lenge den er koblet til en strømkilde. Reserveløsningen vil også ved langvarig svikt i betalingssystemet kunne gjøres mer robust gjennom enkelte forbedringer (Finans Norge, 2017, vedlegg 2). I tilfellene ved svikt vil da terminalen ved brukersted oppsamle all data knyttet til transaksjon for så sende dataen til innløser av transaksjoner når kommunikasjonen er gjenopprettet. Ved bruk av reserveløsningen skriver terminalen ut to kvitteringer, hvorav en gis til kortholder og en beholdes på brukerstedet. Sistnevnte kan sendes inn for avregning ved tilfeller hvor transaksjonene ikke sendes inn av terminalen (ibid., vedlegg 3). Beredskapen knyttet til kortbetalinger har redundans, med alternative løsninger som ikke er direkte avhengig av hverandre. Generelt kan en si felles for alle løsningene er deres avhengighet av strøm.

BALTUS 2.0-FOIet sentral for økonomisk informasjonsutveksling blant bankene. Løsningen er tett knyttet opp aktiviteter rundt kort- og kontobetalinger (Bits AS, ingen dato(d)). Tjenesten ble relativt nylig utviklet og oppdatert til BALTUS 2.0. Tjenesten er regulert av bankenes tilknytning i Bits AS gjennom medlemskap i Finans Norge eller ved samtykke og i tilfeller særvilkår definert av Bits AS (Bits AS, 2018d, s. 1). En slik adgangsbegrensning er

sentralt for at uvørne aktører ikke tar del i dette delsystemet, sårbarheten i systemet forventes styrket av dette. BALTUS 2.0 er ikke avhengig av noen form for spesiell programvare, noe som gjøre den anvendelig for flere ulike deltakere. Videre har tjenesten ende-til-ende sikkerhet, noe som gjør at meldingsutvekslinger innad i systemet er sikre fra ekstern påvirkning (Bits AS, ingen dato(d)).

Tilgang til eID- og eSignatur tjenesten BankID er regulert av medlemskap i Finans Norge, herunder tilsluttet Bits AS, tillatelse til å drive betalingstjenestevirksomhet og rett til å delta i interbanksystemet. Tjenesten forvaltes forretningsmessig og operasjonelt av Vipps AS. Aktørene tilsluttet regelverket om BankID er de som kan utstede BankID-tjenesten (Bits AS, 2018g, s. 1). Deltakerne kan etablere fellesutstedere for produkt- og tjenesteleveranse av BankID, dette må godkjennes av Bits AS. Deltakerne og fellesutstederne kan benytte seg av underleverandører til produksjon og leveranse av BankID-tjenesten. Valg av underleverandør skal meldes til Bits AS, hvorav Bits AS kan pålegge sikkerhets- og kvalitetskrav til underleverandøren (ibid., s. 4-5). Det foreligger en rekke underleverandører som tilbyr tjenesten, støttefunksjoner, optimalisering i henhold til bransje (BankID, ingen dato(a)). Tjenesten og dets mange potensielle underleverandører presenterer en helt egen verdikjede bankene må styre i henhold til å yte tilstrekkelig sikkerhet. Samtidig foreligger det dokumentasjon på flere tilfeller med bortfall av BankID, noe som skaper vanskeligheter knyttet til autentisering av person og signering over nett og ved betalinger (Finanstilsynet, 2018, s. 7; NOU 2015:13, s. 175). En av svakhetene avdekket ved tjenesten, er dets kapasitet. BankID har opplevd flere hendelser på dager med høy belastning (Finanstilsynet, 2018, s. 7). Avvik og hendelser knyttet til BankID kan, grunnet dets mange underleverandører og tilknytning til mobil og mobiltjenester (ibid., s. 30), ha mange årsaker. Kompleksitet i verdikjeden er noe mange av foretakene har presentert som en problematikk knyttet til tjenester i betalingsformidlingen, deriblant BankID (Finanstilsynet, 2019, s. 55). På brukersiden benyttes sertifiseringstjenesten i tiltakende grad til svindel, problemet er tydelig i nære relasjoner hvor familiemedlemmer kjenner hverandres BankID (ibid., s. 54). BankID AS lanserte i 2017 tjenesten xID10 med enkel pålogging, dette figurerer som et supplement til den eksisterende tjenesten (Finanstilsynet, 2018, s. 14). Løsningen kan skape mer redundans knyttet til sertifisering av brukeren. xID10 figurerer dog ikke som en sertifiseringstjeneste på lik linje som BankID (BankiD, ingen dato(b)).

Betalingstjenester

De felles betalingsmuligheter banker kan formidle har også begrensninger til deltakelse fastsatt av Bits AS. Herunder favner AutoGiro, AvtaleGiro, eFaktura og BankAxess.

Regler fastsatt for AutoGiro og AvtaleGiro gjelder alle banker som tilbyr tjenestene (Bits AS, 2018h, s. 1; Bits AS, 2018i, s. 1). Sentralt for tjenestene er fullmakten fra brukeren, begge tjenestene krever at betaler har inngått avtale med betalingsmottaker for at bankene skal kunne initiere belastning, ved AutoGiro, eller debitering, ved AvtaleGiro, av betalers konti. I AutoGiro-tjenesten er vilkåret knyttet til betalingsfullmakt fastsatt i Finansavtaleloven (1999) § 26 (Bits AS, 2018h, s. 2). Bruk av AvtaleGiro skal ha grunnlag i avtale mellom betaler og betalers bank. Videre skal det foreligge en belastningsfullmakt mellom betaler og betalingsmottaker, fullmakten skal foreligge for hver betalingsmottaker og hvert belastningsgrunnlag postulert av betalingsmottaker (Bits AS, 2018i, s. 2). Kravene som foreligger for initiering av transaksjoner knyttet til betalingstjenestene presiserer grunnlaget for formidling av betalinger, og at det ligger hos betaler og deres fullmakt. Videre presenterer reglementene krav for håndtering av tilfeller ved tilbakebetaling, feil og dokumentasjon av fullmakter (Bits AS, 2018h, 2018i). Et slikt detaljert reglement begrenser og reduserer mulighetene til svindel ved betalingskrav. Betalingskravet eFaktura kan ytes av alle banker tilknyttet Bits AS gjennom Finans Norge og som har nettbank, som muliggjør presentasjon og initiering av betaling gjennom digital plattform. Øvrige banker, utenlandske kredittforetak og betalingsforetak kan med samtykke fra Bits AS tilslutte seg til reglene (Bits AS, 2019, s. 1).

Begrensningene knyttet til tilbydere av betalingstjenestene er en risikoreduserende mekanisme knyttet til særlig svindel og misbruk. Tjenestetilgangen som i stor grad defineres av Bits AS er hensiktsmessig og sentral for at tillit til bankene ikke undergraves fra aktører som ikke har tilstrekkelig sikkerhet knyttet til sine løsninger. Herunder vil bankenes selvregulering fungere som sårbarhetsreduserende i den forstand at tilbyderne av tjenestene er underlagt en rekke krav presentert i «Blåboka» (Bits AS, 2018m). Fra Bits AS side presenteres det en også krav knyttet til autentisering og godkjenning av fullmakt fra brukerens side. Svindel kan dog forekomme i tilfeller hvor betaler blir svindlet gjennom alternative kanaler, eksempelvis gjennom phising, sosial manipulering etc. se kapittel 5.2.3. for mer. De mange alternativene som i dag foreligger for brukeren til å kunne gjennomføre betalinger, gjør betalingssystemet som en helhet mindre sårbart (Finanstilsynet, 2017a, s. 46).

En kan si at interbanksystemet, andre FOIer og fellesbetalingstjenester i stor grad kan vurderes som relativt lite sårbart. Mange betalingstjenester, multiple driftslokasjoner,

reserveløsninger og streng adgangsregulering knyttet til bruk av FOIer og betalingstjenester indikerer at betalingsformidlingens har tilstrekkelig redundans og ergo evne til å operere selv under stressituasjoner. Tabellen under illustrerer ansvarsforhold og operatøransvar knyttet til de ulike tjenestene. Av dette kan en se en konsentrasjon rundt noen får leverandører, en slik konsentrasjon kan vise seg problematisk og kan ansees som en sårbarhet dersom en eller flere av disse bortfaller.

Tabell 6, driftsoperatører i sentrale funksjoner i norsk betalingsformidling

FOI/Sentrale betalingstjenester	**Konsesjonshaver**	**Driftsoperatør**
NBO	Norges Bank	Evry Norge AS
NICS	Bits AS	NNI
BankAxept	Vipps AS	NNI
BankID	Vipps AS	Nets AS
BALTUS 2.0	Ikke konsesjonsbelagt	NNI
eFaktura	Ikke konsesjonsbelagt	Nets AS
AutoGiro	Ikke konsesjonsbelagt	Nets AS
AvtaleGiro	Ikke konsesjonsbelagt	Nets AS

5.2.1.2 Sårbarhet knyttet til bankene

Finansforetaks tillatelse til å drive tjenester tilknyttet finansforetak er omfattet av Finansforetaksloven (2015, kapittel 2). Allerede er det kjent at foretakene er tett sammenvevd i flere løsninger for betalingsformidling, så gitt studiens omfang blir det ikke hensiktsmessig å vurdere hver enkelt banks eksponering for sårbarheter. Til tross må det poengteres at foretakene er eksponert i ulik grad. Eksponeringen kan skyldes deres ressurser, samarbeid, underleverandører og lignende strategiske valg. Felles for alle bankene er sårbarhet knyttet til likviditet i henhold til avregning og oppgjør i NICS og NBO.

> *En annen sårbarhet i betalingsformidlingen er selvfølgelig dette her med det likviditetsstyringen i seg selv, det er klart at bankene må ha penger. Som er der til enhver tid, hvis ikke stopper betalingsformidlingen opp. (Informant 41).*

Likviditetsstyring av bankenes konti i NBO er sentral for at betalingsformidlingen skal kunne fungere hensiktsmessig. Herunder foreligger det krav, fastsatt av Bits AS for håndtering av tilfeller hvor banker kan ha likviditetsproblemer og i verste fall være insolvente. Mer om dette i kapittel 5.2.1.4.

Målrettede angrep

Videre oppleves norske banker å være robuste og ha tilstrekkeligsikkerhet mot svindlerangrep (Finanstilsynet, 2018, s. 16). En konsekvens foretakenes robusthet er at teknisk svindel, hvor en bryter barrierene i en nettbank, er mindre i omfang. Svindlerangrep er ventet å ta en tradisjonell form, hvor en manipulerer kundene (ibid.). Fokuset på svindel har vært tilstedeværende hos bankene og gjennom løsninger som BankID blitt sterkt redusert.

> *For en periode hvor det var litt svindel, 8-10 år siden, så ble det jo tatt aksjoner hos bankene og det som var BankID og så videre for å stoppe det opp. Så det som går på svindel nå, går veldig mye på å lure koder fra bruker og mail hvor de gir seg ut for å være andre, ikke direkte tekniske angrep, men mer for å gi seg ut for å være andre aktører mot enkeltpersoner. (Informant 21).*

De tekniske løsningene bankene sitter på i dag gjør angrep fra svindlere lite attraktivt med tanke på det potensielle utbyttet (Finanstilsynet, 2018, s. 16). Dog er risikoen for andre digitale angrep mot bankene tiltakende og beredskapen ved bortfall av viktige løsninger er ikke tilstrekkelig vurdert (Finanstilsynet, 2017a, s. 5). Samtidig er det identifisert at beredskapsløsningene som foreligger ikke er tilstrekkelig uavhengig det eksisterende systemet for betalinger (Finansdepartementet, 2018a, s. 89).

Tjenestedrift

En annen felles sårbarhet for bankene kan være deres avhengighet av IKT. Dyptgående avhengighet av IKT for tjenesteleveranse gjør betalingssystemet sårbart ovenfor utilsiktede og tilsiktede hendelser (Norges Bank, 2018d, s. 14). Gjensidig tilknytning til felles systemer og hverandre er noe som øker sårbarheten da det kan medføre kaskadeeffekter (ibid., s. 25).

> *Det som jeg ser som en sentral sårbarhet er dette med utkontraktering og konsentrasjon av IT-leverandører og det finansielle systemet. Det ene er jo det at det at finansinstitusjoner har outsourcet både drift og utvikling. Noe som gjør at man på den ene siden vil ha større utfordringer knyttet til kontroll på de systemene som er basis for tjenestene. (Informant 11).*

Av kapittel 5.2.1.1 er det bevist at drift av en rekke FOIer er konsentrert rundt et fåtalls leverandører. Bankenes outsourcing viser en lignende tendens hvor vesentlige deler av den operasjonelle driften av systemer og tjenester er konsentrert rundt noen få IT-selskap (NOU 2015:13, s. 170). Samtidig er en av driftslokasjonene for systemene samlokalisert på en plass med en rekke andre, dette skaper en konsentrasjonsrisiko for leveranse av bankenes funksjoner og tjenester (Norges Bank, 2018a, s. 7, 28). Eksempelvis kan en se nivå-1 bankene som outsourcet drift av sine oppgjørssystem til en av de større IT-selskapene. Bankene, DnB og Sparebank 1 SMN, gjør sammen oppgjør for 101 andre nivå-2 banker (ibid., s. 29).

På en annen side er det sånn at jo flere aktører som bruker samme tjenesteleverandør, så øker sårbarheten dersom noe skulle skje. (Informant 41).

Konsentrasjonsrisikoen som foreligger da bankenes funksjoner og drift av FOIer ligger hos samme leverandører skaper en sårbarhet (Norges Bank, 2018a, s. 7; NOU 2015:13, s. 175). Knyttet til FOIene er dog outsourcing av drift av funksjon og drift i stor grad gjort i etablerte og kjente former.

> *Når det gjelder outsourcing vil det kanskje være i infrastrukturen mellom bankene først og fremst. Og der er det fragmentert. Og der er man veldig etablert i betalingsnettverk og struktur, tror kanskje ikke outsourcing påvirker verdikjeden. (Informant 11).*

Verdikjeden

Bankenes videre tiltakende tendens til å outsource oppgaver skaper utfordringer og kan utvikle sårbarheter utover konsentrasjonsrisiko. Utstrakt outsourcing blant bankene, deres IT-leverandører og andre relevante underleverandører skaper en verdikjede som stiller krav til styring (Finanstilsynet, 2019, s. 31). Samhandling mellom de ulike aktørene som deltar i verdikjeden er sentralt for å kunne levere betalingstjenester og håndtere avvik tilstrekkelig for sluttbrukeren.

> *Outsourcer man, vanskeligere å få tak i de man skal snakke med kanskje, kanskje ikke kompetansen er der man vil at den skal være. Og er den i utlandet, vi vet ikke hvordan sikkerheten er, hvordan er risikovurdering. Du har en annen risikovurdering på noe du har in-house eller i nærheten enn noe du har for eksempel i utlandet eller at du kjøper det fra en datasentral som du ikke har kjøpt fra før. (Informant 22).*

Sitatet viser til et styringsdilemma, ved avvik på tjenesten som er satt ut kan det være problematisk å kunne kontrollere eller gjenopprette systemet. En problematikk knyttet til outsourcing kan tillegges styringsdimensjonen, og at foretak ved outsourcing av tjenester eller støttefunksjoner har problemer knyttet til tjenesteleveranse (Finanstilsynet, 2018, s. 8). Outsourcing kan videre komplisere verdikjeden og i tilfeller gjøre den lang og uoversiktlig (NOU 2018:14, s. 20). Gottschalk (2013, s. 17) har også identifisert at kompleksitet kan medføre at bankenes aktiviteter ikke lenger kan sees i en lineær og etterfølgende verdikjede, noe som gjør styring av verdikjeden vanskelig. Et ytterligere problem ved uoverskuelighet i verdikjeden er problematikk i å identifisere kritiske komponenter. Problematikken rundt manglende kjennskap til egen verdikjede er noe Finanstilsynet (2018, s. 20) har trukket frem. Her poengteres at bankene ikke i tilstrekkelig grad inkluderer slike vurderinger i sine interne risikoanalyser.

Avtaleinngåelse og styring av funksjoner

Avtalene som inngås ved utsetting av tjenester og funksjoner burde i avtale med underleverandører inneholde plan for styring, leveranse, sikkerhet og beredskap (EBA, 2018, s. 16; Finanstilsynet, 2019, s. 9). Til tross for at det foreligger en rekke anbefalinger for forhold som burde avklares og inkluderes i slike avtaler, er det flere problemer knyttet til styring av verdikjeder hvor det er outsourcet (Finanstilsynet, 2018, s. 20). Jo flere aktører som inkluderes i verdikjeden jo mer kompleks blir verdikjeden og ergo vanskeligere å styre. Herunder blir det derfor sentral for virksomheten å kartlegge alle delene som inngår i verdikjeden og avdekke hva i verdikjeden som er kritisk (EBA, 2018, s. 17). Et videre aspekt ved outsourcing er manglende tilgangsstyring hos foretakene. Dette er å regne en som sårbarhet da medarbeidere hos underleverandører kan gjennom overtakelse av tjenester ha inngang og tilgang til kritiske systemer (Finanstilsynet, 2019, s. 26). Utilstrekkelige avtaler knyttet til outsourcing kan indikere at foretakene har manglende bestiller-kompetanse, noe som medfører at krav kan utelates fra avtalen (Finanstilsynet, 2019, s. 31). Videre kan manglende oppfølging fra foretakenes side på etterlevelse av avtalen også være problematisk. Problemet ved avtaleinngåelse synes å være mer pressende for mindre foretak (ibid.).

> *Men det at det blir en økt grad av utkontraktering og at det blir flere tjenesteleverandører gjør at mange tjenester i seg selv blir noe mer komplekse og at samhandling, når flere aktører skal samhandle så utgjør også det en risiko i seg selv. Særlig om de må samhandle dersom hendelser skjer, så det vi er opptatt av er at det er trukket opp gode rutiner for håndtering av hendelser mellom leverandører. Og ikke bare mellom kjøper av tjenesten og leverandøren. (Informant 41).*

Samhandling er også noe som kan forventes å bli en utfordring som en følge av outsourcing, særlig ved tilfeller hvor avtaler ikke er tilstrekkelige. En slik vurdering kan begrunnes med at mangler i avtaleinngåelser synes å være en trend (Finanstilsynet, 2019, s. 26).

Trenden knyttet til outsourcing og dets effekt på manglende oversiktlighet i økosystemet for betalinger er noe som potensielt vil øke risikoen i systemet (NOU 2015:13, s. 176). Problematikken blir mer prekær i tilfellene hvor tjenesten er satt offshore til utenlandske aktører (Finanstilsynet, 2019, s. 72).

> *.. Vi driver outsourcing ved at vi sender ut utviklingsoppdrag hos andre. Det dette har ført til, er egentlig at det har blitt mer fokus på sikkerhet og utvikling. Vi kan ikke tillate at de får tilgang til produksjonssystemer, det er jo helt uaktuelt, og tilgang til reelle data sånn at personer utenfor Norge får tilgang til reelle testdata er heller ikke aktuelt. Så krav til personvern og sånne ting har ført til at det er mer fokus på sikkerhet i egen organisasjon når vi skal bruke ressurser som ikke sitter lokalisert i våre egne lokaler. (Informant 21).*

Informant 21 belyser hvordan sin herværende organisasjon benytter seg av offshoring for utvikling av tjenester. Det oppleves av informanten at fokuset på sikkerhet øker i tilfeller ved outsourcing. Foretak benytter seg særlig av offshoring for IKT-tjenester og brukersupport. Offshoring kan bidra til økt innovasjon og produktutvikling for foretaket (Gottschalk, 2013, s. 25). Dette kan medføre at mer profesjonelle og effektive aktører overtar ansvar for disse oppgavene (ibid.). Tjenestene kan i så måte bli mer stabile og reliable. Samtidig vil tjenestene og oppgavene som outsources være utenfor foretakets kontroll og styring. Geografisk avstand er også en sårbarhet som kan tillegges outsourcing, hendelser langt unna kan skape ringvirkninger for foretaket (Finanstilsynet, 2019, s. 47-48). Betydelig avhengighet av underleverandører er da problematisk for foretak i Norge. Eksterne hendelser som ikke rammer foretaket direkte kan få signifikante ringvirkninger for deres operasjonelle og konsesjonsbelagte tjenester. I tilfeller tjenester outsources og eller offshores til eksterne underleverandører, er det hensiktsmessig for foretakene med personell med kompetanse til videre drift av tjenesteutsatte løsninger (ibid.). Samhandlingsproblemet kan bli mer prekært ved offshoring, her vil faktorer som kulturelle forskjeller, språk, geografisk avstand og kunnskapsoverføring være utfordrende (Gottschalk, 2013, s. 26). En kan derfor i pressende situasjoner oppleve at kommunikasjonskanalene mot underleverandørene ikke fungerer hensiktsmessig. I slike situasjoner hvor det ikke foreligger tilstrekkelig etablering av kommunikasjon vil opprettholdelse og eller gjenopprettelse av funksjonen bli problematisk (Finanstilsynet, 2019, s. 55). Avvik i bankenes funksjoner kan videre få innvirkning for andre funksjoner som inngår i betalingsformidlingen ved kompetansefrafall.

> *Fra NICS sin side, det at banker outsourcer sin drift, sin betalingsformidling kan skape flere feil, usikkerhet og ustabilitet. Grunnen til det er at man stort velger sentraler som gjør flere oppgaver for flere, kanskje med de samme ressursene. Jeg tror at det bli mindre kompetanse og vanskeligere å nå gjennom for å søke om hjelp og råd. (Informant 22).*

Situasjoner ved hendelser eller avvik av funksjoner kan kreve økt behov for kommunikasjon med andre relevante aktører. En konsekvens av manglende styring kan være at kommunikasjon vanskeliggjøres som en følge av at ulike leverandører og tjenesteytere i verdikjeden opererer med ulike prosesser og kanaler for kommunikasjon.

> *(..)Det at det blir en økt grad av utkontraktering og at det blir flere tjenesteleverandører gjør at mange tjenester i seg selv blir noe mer komplekse og at samhandling, når flere aktører skal samhandle så utgjør også det en risiko i seg selv. Særlig om de må samhandle dersom hendelser skjer, så det vi er opptatt av er at det er trukket opp gode rutiner for håndtering av hendelser mellom leverandører. (Informant 41).*

I komplekse verdikjeder blir derfor informasjonsutveksling og gode kanaler for kommunikasjon viktig for tjenestens funksjonalitet (Finanstilsynet, 2019, s. 55). Kommunikasjon nevnes også av Gottschalk (2013, s. 27) som faktor for suksessfylte outsourcingsavtaler. God kommunikasjon til sine underleverandører vil også kunne forenkle foretakenes styring av verdikjeden. Et videre aspekt er knyttet til kunnskap og kompetanse som kan bortfalle i foretakene. Dette kan på sikt utvikle seg til å bli en sårbarhet som må adresseres av foretakene for å kunne opprettholde tilfredsstillende tjeneste- og sikkerhetsnivå.

5.2.1.3 Trusselbilde

Trusselbilde knyttet til betalingsformidling har ifølge flere informanter endret seg med årene, informant 22 poengterer.

> *Nå har vi kjørt risikoanalyser i alle år, det er ganske spennende å se hvordan risikobilde har endret seg.* (*Informant 22).*

Av kapittel 5.2.1.2 er det identifisert hvordan bankene gjennom økt robusthet og nye løsninger har endret trusselbildet knyttet til svindel (Finanstilsynet, 2018, s. 16). Trusselbildet er dog ikke noe som forsvinner, men heller noe som endrer seg. Behovene for at bankene i større grad forbereder og gjør seg kjent med egne sårbarheter, i egen infrastruktur og i utkontrakterte tjenester blir større (ibid., s. 6). Finanstilsynet (2018, s. 21) ser samtidig internasjonalt en global økning i cyberangrep mot bankene. Angrepene sikter i større grad mot grunnleggende infrastruktur og manipulering av de som styrer infrastrukturen (Finanstilsynet, 2019, s. 34). Grunnet finansnæringens store digitale plattform er cyberangrep blitt den fremste flaten for ondsinnede handlinger. I et område som er så IKT-intensivt og av viktighet for den finansielle stabiliteten (NOU 2015:13, s. 168), så kan en forvente at trusselbildet mot banker og betalingsformidlingen vil være digitalt. Eksempelvis kan en se Equifax, et amerikansk kredittovervåkningsfirma, som opplevde at 700.000 av sine britiske kunder fikk personlig informasjon på avveie. Deriblant opplysninger knyttet til telefonnummer, kredittkortdetaljer og informasjon knyttet til kundenes førerkort (The Guardian, 2017). Hendelsen med Equifax er et eksempel på tilsiktede hackerangrep, som kontinuerlig preger finanssektoren (Finanstilsynet, 2019, s. 33). Eksempelet illustrerer samtidig hvor viktig personopplysninger knyttet til kundene er. Konsekvensene knyttet til hackerangrep kan resultere i en lignende hendelse som hos Equifax. En kan også vurdere konsekvensene til å favne mye bredere, ergo at banken eller foretaket blir satt ut av ens funksjon (Finanstilsynet, 2018, s. 21). Truslene som omgir bankene antas å være høyest knyttet til angripere som er velorganisert, ressurssterke og besitter betydelig kompetanse (Finanstilsynet, 2019, s. 34).

Bankenes overvåkning av trusselbildet er viktig for beredskapen og det å kunne ta proaktive konsekvensreduserende tiltak. Norske foretaks overvåkningssystemer oppleves tilstrekkelige og har avverget angrep før konsekvensene har blitt alvorlige. Norsk finansnæring vurderes generelt å være godt rustet mot digitale angrep, mye siden sitt arbeid med feltet (Finanstilsynet, 2019, s. 33). I møtet med trusselbildet ble FinansCERT etablert som en organisasjon som skulle hjelpe norske finansforetak med informasjonsdeling knyttet til trusler. Senere er organisasjon blitt sammenslått med tilsvarende nordiske ordninger. I dag har organisasjonen Nordic Financial CERT[24] fire oppgaver knyttet til trusselbildet (Finans Norge, 2019). NFCERTS hovedoppgaver består i overvåkning og informasjonsdeling; support ved hendelser; koordinering av respons på angrep, herunder benyttelse av ressurser i nettverket; og dele informasjon med alle internt i nettverket samt samarbeid med lignende eksterne nettverk (ibid.).

5.2.1.4 Beredskap i betalingsformidlingen.

Generelt om arbeidet rundt beredskap i betalingsformidlingen foreligger det indikasjoner på at foretakene leggere ned betydelige ressurser i sine løsninger. Både knyttet opp mot å redusere sårbarheten, gjennom redundansbygging, men også å avdekke potensielle beredskapsløsninger (Finanstilsynet, 2018, s. 11). NFCERT bidrar til bredt samarbeid og koordinering i møte med truslene innen næringen (Finans Norge, 2019).

> *Norsk finansnæring er veldig godt forberedt og utover det har hver enkelt bank bygget opp ganske effektive organisasjoner for å håndtere cyberkriminalitet. Så har man jo også et samarbeid blant annet gjennom noe som heter FinansCERT, hvor man jobber veldig tett sammen. (Informant 11).*

NFCERT tilrettelegger gjennom sin kommunikasjon og samordning av ressurser (Finans Norge, 2019), for mer hensiktsmessig beredskap blant deltakende foretak. Kunnskapsgrunnlaget og informasjonsdeling vil bedre beredskapsløsningene og redundansen i systemet.

Insolvensbehandling og ramifikasjoner for sluttbrukeren.

Overordnet i bankenes felles betalingsløsninger er det tatt høyde for, gjennom NICS, avvik og hvordan dette kan håndteres. I NICS er det blant annet etablert alternative løsninger for innsending og mottak av transaksjoner i tilfeller ved problemer i kommunikasjonene (Bits AS, 2018f, s. 1). En slik løsning indikerer at det foreligger beredskapsløsninger for bortfall av kommunikasjon om transaksjoner. Samtidig foreligger det også ulike løsninger knyttet til

[24] Siden betegnet som NFCERT.

deaktivering av bruttotransaksjoner i NICS og heller benytte seg av nettoløpet for avregning; løsning for stopp av transaksjoner i SWIFT-format; samt løsninger for midlertidig stopp av behandlinger av transaksjoner og midlertidig full stopp av NICS (ibid., s. 1-2).

Likviditetsstyring, jf. kapittel 5.2.1.2, er sentralt for at interbanktransaksjoner skal kunne gjennomføres og sluttbrukeren skal kunne få gjennomfør betalinger og overføringer. En form for beredskap som er lagt inn for å beskytte dette er knyttet til bankenes konti i Norges Bank. Bankene kan følge sin posisjon for å styre likviditeten gjennom informasjonssystem som er NICS Online (Bits AS, 2018b, s. 1). Ved tilfeller hvor banken ikke har dekning for sin posisjon i NBO foreligger det en prosess for avvikshåndtering. Første steget i prosessen er at det varsles angående manglende dekning til gjeldende bank. Resterende banker får så informasjon om at nettoavregningen er i kø grunnet manglende dekning hos en av deltakerne (ibid., s. 2). Neste trinn i prosessen er knyttet til tilfeller hvor en nettoavregning i NICS avvises grunnet manglende dekning. I slike tilfeller vil banken få status som midlertidig sperret (Bits AS, 2018k, s. 1). tredje steg i prosessen for avvikshåndtering er en redegjørelse fra banken som har status midlertidig sperret, herunder skal banke eksplisitt opplyse hvorvidt om det har finansiell kapasitet til å videre delta i NICS (Bits AS, 2018b, s. 2). Påfølgende i prosessen vil bankens BankAxept-instrument og dens tilgang til Straksbetalinger sperres og avvikles i tilfeller hvor Bits AS finner av bankens egenvurdering grunnlag for det, herunder vises det til at banken selv må eksplisitt opplyse om deres egnethet til å delta i NICS på normal vilkår (ibid., s. 3). Siste steget i prosessen omhandler når en bank settes under offentlig administrasjon, her skal banken få status som «under offentlig administrasjon. Dette medfører at banken ikke lenger deltar i NICS og alle uoppgjorte transaksjoner skal avvises, herunder inkluderes ikke BankAxept og straksbetalinger (ibid.).

Det foreligger en særegen BankAxept-avtale ved hendelser hvor en av deltakerne i avregningen er satt under offentlig administrasjon eller er blitt insolvent (Bits AS, 2018j, s. 8). Herunder presiseres det hvordan bankens BankAxept-transaksjoner skal gjøres opp. Bankens uoppgjorte posisjoner skal gjøres opp med eventuelt avsatte midler. Om avsatte midler ikke eller delvis dekker opp uoppgjorte BankAxept-transaksjoner skal de utestående uoppgjorte transaksjonene dekkes av deltakende banker. De deltakende bankene skal da dekke den negative posisjonen til insolvent bank, beregningen her baseres på antall utstede BankAxept-instrument 31.12 forhenværende år (ibid.). En slik mekanisme knyttet til behandling av aktører under offentlig administrasjon eller insolvensbehandling vil ikke nødvendigvis vurderes som beredskap for deltakerne. I en større samfunnsmessig perspektiv kan en dog se

hvordan kunder som normalt ville vært berørt av ens bank manglende evne til å føre sine funksjoner, ikke i like stor grad blir akutt berørt.

Kundenes betalingsevne ved bortfall av elektroniske betalingsløsninger

I sentrale betalingsløsninger som BankAxept er det avdekket at det foreligger en reserveløsning i de tilfeller kommunikasjonslinjene faller bort (Finans Norge, 2017, vedlegg 3). Generelt er det også avdekket at foretakene legger ned vesentlig arbeid i reserve- og beredskapsløsningene i løsningene sine. Tilgjengeligheten på tjenestene er derfor blitt bedre (Finanstilsynet, 2019, s. 13). Bankenes generelle arbeid knyttet til beredskap har dog mangler knyttet til styrende dokumenter, tester, øvelser, trening og kriseløsninger. Deres potensielt manglende evne til å reagere ved hendelser av stort omfang er derfor noe øker risikoen for vesentlige problemer og skader (ibid., s. 22). Testingen av eksisterende kriseløsninger er heller ikke gjort tilstrekkelig av flere parter. Ergo er det knyttet usikkerhet til om løsningene er tilstrekkelige ved hendelser (ibid., s. 24). Usikkerhet kan også til dels tillegges at det har vært manglende hendelser som testet kriseløsningene. Ansvaret for tilstrekkelige løsninger, vurdering av deres og organisasjonens kapasitet samt sikre samhandling med relevante leverandører ligger hos foretakene (ibid., s. 35). Beredskapsløsningene som eksisterer i betalingsformidlingen vurderes samtidig som ikke tilstrekkelig segregert fra de allerede eksisterende løsningene (Finansdepartementet, 2018a, s. 88-89).

Kontantberedskap for bortfall av elektroniske betalingstjenester.

Beredskap knyttet til potensielle bortfall av de elektroniske tjenestene er noe Finanstilsynet og Norges Bank i større grad har etterlyst. I sin årlige ROS-analyse poengterer Finanstilsynet (2017a, s. 11) at beredskapen knyttet til den elektroniske betalingsformidlingen hos bankene ikke var tilstrekkelig. Av Stortingsmelding 14. 2017-2018: *Finansmarkedsmeldingen 2018* kommer det samtidig frem at det ikke eksisterer beredskapsløsninger som er tilstrekkelig uavhengig av det vanlige betalingssystemet (Finansdepartementet, 2018a, s. 89). Dette betyr at konsekvensene ved potensielle svikt i det ordinære betalingssystemet også vil kunne sette beredskapsløsningen ute av spill.

> *Det jo også sagt at forbedring av beredskapen i det elektroniske betalingssystemet kan legges til grunn når man skal se på kontantberedskapen. Så jo bedre og mer omfattende beredskapen i det elektroniske er, jo lavere nivå kan man legge på beredskapsløsninger for kontantdistribusjon. Og så er det sånn at jeg er usikker på om det kommer opp noe elektronisk alternativ, som kan være mer avhjelpende enn kontanter. (Informant 41).*

I møte for denne manglende beredskapen er kontantberedskap blitt et aktuelt tema. Kontanter er fortsatt tvungne betalingsmidler i Norge (Norges Bank, 2018b, s. 69), dette kommer frem i Finansavtaleloven (1999, § 38-3). Innføringen av Finansforetaksforskriften (2017, § 16-7), gjør bankene juridisk bundet til å ha løsninger for å håndtere en uforutsett økning i etterspørsel av kontanter. Dette er myndighetenes respons på det de oppfatter som manglende beredskap i de elektroniske betalingsløsningene (Finansdepartementet, 2018a, s. 89; Finanstilsynet, 2017a, s. 10-11). I forkant av innføring § 16-7 i Finansforetaksforskriften (2017) forelå det en diskusjon initiert av Norges Bank og Finanstilsynet. I høringsnotatet understrekes det at manglende beredskap knyttet til elektronisk betalingsformidling i Norge, gjør det nødvendig med kontantberedskap (Finanstilsynet & Norges Bank, 2016, s. 4). Videre vises det til at bankene står til ansvar for at det skal kunne distribueres kontanter til kundene. Av informant 11 poengteres det en problematikk knyttet til kontantdistribusjon:

> *Det er det jo egentlig bankene som er pålagt av myndighetene til å skulle ivareta kontantdistribusjon. Du kan si det normalt er gjort gjennom filialnettverket til bankene, eller ved hjelp av kontantautomater og minibanker og slikt. Bankene har nå bygget ned filialnettverket og også i mindre grad kontantautomater så vil det kunne være en sårbarhet dersom elektroniske betalingsløsninger faller ned over lengre tid at det kan bli vanskelig å få til effektiv distribusjon knyttet til kontaktbehovet. (Informant 11).*

Problematikken vedkjennes av Finanstilsynet & Norges Bank (2016, s. 6), men meddeler at kostnadene knyttet til dette må avveies mot sårbarhetsreduksjonen dette vil medføre. Finans Norge (2017) har i sitt høringssvar i forkant av implementeringen av § 16-7 i Finansforetaksforskriften (2017) presentert deres og i så måte bankenes syn på innføringen. I høringssvaret illustreres det at bakgrunnen for innføring av § 16-7 i Finansforetaksforskriften mangler presise forklaringer på hvilke aspekt av beredskapen knyttet til dagens system for betalingsformidling som ikke er tilstrekkelig. Samtidig understreker også deres syn på dagens elektroniske betalingstjenester, som de anser som robust (Finans Norge, 2017, s. 2). I tilknytning til BankAxept så presenteres også systemets alternative løsninger som vil fungere til tross for sviktende kommunikasjon mellom brukersted og FOI og eller bank (Finans Norge, 2017, se vedlegg 3). Løsningen har kun behov for elektrisitet og at terminalen betjenes av en representant tilknyttet brukerstedet. Ved bruk av reserveløsningen så vil terminale produsere to kvitteringer, en med til kunde om at transaksjonen er gjennomført og en hvor brukerstedet vil ha informasjon om transaksjonen. Brukerstedet vil ved forespørsel formidle brukerstedsbanken med relevant informasjon som skal benyttes til oppgjør om transaksjonsdataen ikke blir videresendt fra terminalen (ibid.). Ved kommunikasjonsbrudd så

vil heller ikke det kunne være mulig for minibanker å fungere da de ikke får kommunisert med brukers bank, bankene vil ha problemer med å uthente kontanter fra depoter og Norges Bank vil heller ikke kunne overføre kontanter uten autorisasjon (ibid., s. 5). Finans Norge (2017, s. 4) knytter så problematikken opp mot elektrisitet, hvor kontantapparat og kassasystemer i de aller fleste tilfeller også er tilknyttet og avhengig av strøm. Så bortfall av elektroniske betalingstjenester som en følge av strømbrudd vil også innvirke på kasseløsningene ved brukerstedene noe som medfører at beredskapen ved bortfall må belage seg på den eksisterende kontantbeholdningen hos brukerstedet gitt tidspunktet for strømbrudd. Bruk av kontanter ved tilfellet ville samtidig bestride sikkerhets- og regnskapsmessige krav som stilles til brukerstedet (ibid.).

5.2.2 Potensielle nye sårbarheter

Store endringer er ofte forventet å medføre nye og endrede risikoer og sårbarheter (Finanstilsynet, 2018, s. 11). En generell bemerkning er at store endringer i seg selv presenterer en risiko for betalingssystemet (ibid.). Endringer har særlig vært forventet ved et mer spredt aktørbilde og benyttelse av nye teknologiske løsninger (ibid., s. 41-44). Et nytt og bredere aktørbilde kan samtidig også medføre en endret risiko som integreres inn mot bankenes tjenester og ergo brukerne (ibid., s. 11). Drivkreftene bak endringene er forventninger til tjenester, teknologiske fremskritt og nye aktører noe som har medført endringer i reguleringene (Finanstilsynet, 2018, s. 11).

Sårbarheter som en følge av implementering av PSD2

I ROS-analysen for 2017 poengterer Finanstilsynet (2018, s. 15) at nye aktører som en følge av PSD2 forventes å etablere betalingstjenester i Norge. Tilsvarende analyse fra 2018 presenterer et litt annet syn. Grunnet de strenge reguleringene som foreligger i direktivet forventes det en mer moderat pågang av aktører (Finanstilsynet, 2019, s. 16).

> *Det PSD2 var skrevet og ment for å gjøre var å lage et sikrere system men samtidig å åpne for konkurranse ved å fjerne en del av de barrierene som bankene har bygget rundt sine tjenester. For å gi bedre tjenester og vilkår til brukerne, det var det PSD2 i utgangspunktet var ment til å være. Det det nå har blitt gjennom intens lobbyering fra de mer etablerte aktørene, er en veldig strupet og begrenset effekt. Eksempelvis var det meningen at alle bankkonti skulle åpnes og at tredjeparter skulle aksessere det gjennom samtykke fra brukeren, nå er det begrenset ned til kun personkonti og lønnskonti. Ikke lånekonti, ikke pensjons- og sparekonto. Det vil ikke ha den samme effekten og de som tjener mest på det her nå er nok de etablerte aktørene, hvert fall de som velger å benytte seg av muligheten til å få større distribusjonsnettverk gjennom å åpne opp gjennom open banking. (Informant 31).*

Synet presentert av informant 31, som figurerer som en av de nyere aktørene på betalingsmarkedet, er også noe som understøttes av mer etablerte aktører. Tilgangen tredjepartsaktører som får gjennom grensesnittene utviklet i tråd med PSD2 omfatter betalingsinitiering og kontoinformasjon (Norges Bank, 2017, s. 9; PSD2, 2015, Artikkel 66 og 67). Artikkel 66 i PSD2 (2015) beskriver hvordan tredjepartsaktører kan, med samtykke og initiering fra brukeren gjennomføre betalinger. I Artikkel 67 gir tredjeaktører adgang til å benytte kontoinformasjon i tjenestetilbudet sitt. Samtidig poengteres det at aktører som yter betalinger ikke skal belaste brukeren tilleggsgebyr for å initiere betalinger via en tredjepartsaktørs betalingstilbud (PSD2, 2015, Artikkel 62).

Tilgangen nye aktører oppnår gjennom PSD2 er derfor forventet å være begrenset og en kan derfor spørre seg hvorvidt slike aktører er å anse som en sårbarhet for betalingsformidlingen. Tredjepartsaktører, grunnet deres begrensede tilgang, er ventet å legge seg utenpå bankenes eksisterende løsninger. En slik vurdering legges til grunn hovedsakelig grunnet deres tilgang gjennom bankenes standardiserte grensesnitt (PSD2, 2015, Artikkel 66 & Artikkel 67). PSD2 stiller samtidig strenge krav til aktørene som ønsker tilgang til grensesnittene, kravene som stilles medfører at aktørene som får tilgang oppleves å ha tilstrekkelig sikkerhet i sine løsninger (Finanstilsynet, 2019, s. 16).

> *Det er åpent for alle som har fått konsesjon, det er et av kravene i loven er at det ikke må foreligge noen avtale mellom tredjepartsaktøren og banken. Det vi gjør der er at loven krever at disse tredjepartsaktørene skal få konsesjons hos tilsynsmyndighetene og basert på denne konsesjonen kan de da få tildelt et digitalt sertifikat som de kan bruke da for å identifiseres seg mot banken. Og vi er pålagt å sjekke at det sertifikatet for å være sikker på det er en aktør som da har en konsesjon til å knytte seg opp mot bankene. (Informant 11).*

Bankene har også et ansvar knyttet til å inspisere de utstedte sertifikatene hos nye tredjepartsleverandører. Ansvaret for kundens sikkerhet tillegges ved bruk av aktører knyttet til PSD2-grensesnittet i en viss grad bankene (Finanstilsynet, 2019, s. 49). Herunder påligger det et ansvar knyttet til at bankene har utviklet tilstrekkelig sikkerhet i forhold til både tredjepartsaktøren og kunden som benytter tredjepartsaktørens løsninger. En kan til tross for strenge regulatoriske krav tenke at nye aktører knyttet til betalingsformidling som en kanal for målrettede angrep mot bankene. Sårbarheter knyttet til tredjepartsaktørens løsninger og forsøk på svindel av brukerne trekkes frem som mulige fremgangsmåter (ibid.).

Så lenge de er regulert så skal en ikke tro at typiske tredjepartsaktører i forbindelse med PSD2 har noen dårligere løsninger og dårligere sikkerhet enn eksisterende. Fordi de skal tilfredsstille lover og regler, de skal gis konsesjon, de skal demonstrere at de har på plass rutiner og prosesser før de får konsesjon. (Informant 41).

En kan derimot grunnet den strenge reguleringen som nye tredjepartsaktører er underlagt ikke konkludere med at aktører gjennom PSD2 vil bidra til økt sårbarhet, utover økt eksponering. Bankene og deres verdikjeder kan ventes å bli noe mer utsatt som en følge av større eksponering, en kan derimot ikke trekke samme linjer for interbanksystemet.

(..) PSD2-messig for avregningsentralen, foreløpig så ser jeg ikke noe potensiell risiko rundt det. Men vi vet jo at ting på kommer til å endre seg på en eller annen måte. (Informant 22).

Interbanksystemet forventes ikke direkte berørt av en nytt og bredere aktørbilde i norsk betalingsformidling. Aktører som ønsker å ta del i avregning og oppgjør i NICS og NBO må ved et slikt ønske få konsesjon til å drive bankvirksomhet gjennom Betalingssystemloven (1999, kapittel 5) og Finansforetaksloven (2015, kapittel 2) og dernest medlemskap i FNO eller særskilt tillatelse av Bits AS (Bits AS, 2018c, s. 2).

Open banking, manglende regulering - manglende sikkerhet?

Nye aktører er ikke utelukkende knyttet til grensesnittene ved PSD2, men aktører kan også gjennom open banking inngå bilaterale samarbeid med banker. Herunder kan det foreligge andre avtaler og alternative grensesnitt som vil presentere andre muligheter for tredjepartsaktøren involvert (Finanstilsynet, 2017a, s. 11). Bruken av open banking-grensesnitt er ikke underlagt reguleringer fastsatt i PSD2, herved er tredjepartsaktørene i mindre grad underlagt reguleringer. Samtidig bør det poengtere at det på europeisk nivå på initiativ fra den europeisk sentralbanken jobbes med å etablere et standardisert scheme for open-banking, som vil gjelde alle aktører (European Central Bank, 2019, s. 1-2). Løsningene, som dog pr. dags dato fortsatt er uregulerte grensesnitt, er allerede noe bankene har begynt, en kan forvente at slike grensesnitt vil være bi- eller multilaterale og i flere tilfeller proprietære. Avtalene kan også i flere tilfeller ventes å gå utover det som er lovfestet i PSD2 (Finanstilsynet, 2019, s. 15). Samtidig poengteres det dog at slike krav burde foreligge i samarbeid mellom tredjepartsaktører og banker samt i utviklingen tilhørende grensesnitt (ibid., s. 49). En kan dog se for seg tilfeller hvor løsninger ønskes å implementeres rask, for å være først ute med brukervennlige løsninger. Slikt fokus kan i tilfeller neglisjere fokuset på sikkerhet og løsningene som da implementeres til markedet kan ha utilstrekkelig sikkerhet.

Så hvis man ser på risiko kan man jo kanskje tenke seg at en aktør for å få noe spennende ut i markedet ikke tar hensyn til sikkerheten på en god nok måte. At nå gjelder det liksom å komme først med de nye betalingsløsningene, eller det kan gjelde innenfor lån eller være innenfor forsikring eller andre ting som ikke er innenfor PSD2. Og så sier man, «nei, kjør på vi prøver» og så glemmer man kanskje sikkerheten. Så jeg tenker nok at open banking kan utfordre sikkerheten hvis ikke bankene er veldig bevist på det. For problemet er da at det blir opp til den enkelte bank og det er ikke sikkert alle banker har like mye fokus eller like mye kompetanse på det. (Informant 21).

Utilstrekkelig sikkerhet i tjenestene som introduseres av nye aktører, sammen med selvdefinerte grensesnitt, og økt angerepsflate nye tredjepartsaktører presenterer kan medføre økt risiko. Her vil tilgangen tredjepartsaktørene får til bankenes infrastruktur være avgjørende for sårbarheten og konsekvensene ved intenderte angrep. Igjen så kan en se til presiseringen gjort av Finanstilsynet (2019, s. 49), om at kravene i PSD2 burde ligge til grunn ved utvikling av grensesnittet utenfor regulering. Informant 21 poengterer at utvikling av grensesnitt knyttet til open banking aktører kan ha et grensesnitt som er annerledes enn de krav som foreligger i PSD2. Dog bør det nevnes at informantene poengterer at sikkerheten ved grensesnittene knyttet til open banking-aktørene også ansees som tilfredsstillende.

Det jeg vil si er at det er veldig fornuftig å følge de samme prinsippene for open banking API som for PSD2. Det er en del rundt sikkerhet i PSD2 som ikke har vært på plass før nå (..) Så det er helt klart at vi har levert grensesnitt som vi mener er sikre (..) Så jeg vil påstå at vi ivaretar sikkerheten og har gjort det tidligere også, men det har vært en annen måte enn ved PSD2 for det har kommet med ekstra krav som skal implementeres nå før sommeren. (Informant 21).

Om utvikling av grensesnitt kan være bekymringsverdig med tanke på sikkerhet vil differensiere. Større aktører som utvikler grensesnitt innehar ressurser, kompetanse og fokus omkring sikkerhet. Ergo kan en i større grad forvente at grensesnittene som gis ut til å være tilstrekkelig sikre. Mindre aktører kan derimot oppleve problemer med dette, grunnet manglende kompetanse, ressurser og bevissthet rundt sikkerhet.

Fintechaktører, foreligger det tilstrekkelige ressurser?

Nye betalingstjenester og nye aktører som introduseres i betalingsformidlingen vil kunne bety en mer effektiv betalingsformidling (Norges Bank, 2019, s. 10). En kan vurdere hvorvidt aktørene som gjennom enten bilaterale lukkede grensesnitt eller PSD2-grensesnitt vil medføre økte sårbarheter i betalingsformidlingen.

Det er ofte spekulert i at lengre verdikjeder og nye aktører skaper ny sårbarhet, min holdning er at så lenge de nye aktørene er regulert så skaper de ikke en annen sårbarhet enn at det er en annen aktør inn i systemet. (Informant 41).

Selv om nye aktører ikke har nødvendigvis sårbarheter ved seg og sine løsninger, presenterer de en større angerepsflate inn mot bankene. Tredjepartsaktører tilknyttet bankene kan bli utsatt for målrettede angrep i forsøk på å svekke bankene og tilhørende betalingstjenester. EBA (2018, s. 8) poengterer hvordan tredjepartsleverandører kan fungere som en kanal for cyberangrep på finansielle aktører. Kriminelle som ønsker å svekke finansforetak og deres evne til å yte tjenester, kan benytte det svakeste leddet i verdikjeden som i tilfeller kan være en mindre fintechaktør.

> *«Phising» ja, ikke sant. Det var ordet jeg lette etter. Dette går jo ikke så mye på betalingssystemer. Så jeg synes kanskje at svindel ikke virker å være et så stort problem, sånn som vi opererer i dag. Dette kan komme litt etter hvert, i og med dette med nye aktører som kanskje kan gi større problemer med det. (Informant 21).*

Svindel kan igjen bli et økende problem for betalingsformidling da målrettede angrep kan sikte på hull i løsningene som leveres av tredjepartsaktører. Herunder vil det derfor være sentralt at i bilaterale samarbeid at bankene som gir tredjepartsaktører tilgang på infrastrukturen sin innehar tilstrekkelig sikkerhet i sine løsninger.

Bigtechaktører, tar de hensyn til eksisterende regelverk?

Inntoget av bigtecher i betalingsformidling er underveis og er ventet til å kanskje med tiden å øke i omfang. Både i form av aktører og tilbud av tjenester. Potensielle sårbarheter knyttet til at slike aktører er ikke nødvendigvis knyttet til utviklingen av løsningene deres.

> *Jeg tror ikke nødvendigvis Facebook, Microsoft eller Google er noe dårligere sikkerhetsmessig for å si det sånn. Nå skal jeg kanskje være litt forsiktig med å si Facebook, for der har det vært noen sikkerhetstematikk. Men om du ser på Google og Microsoft så er de stort sett en gjennomsikre og solide, de lever av sikkerhet. Jeg vil tro at de går inn på betalingstjenesteområder også og andre områder igjen av å bare være betalingsinitiator som Apple Pay. Apple Pay, som jeg sier de trenger ikke konsesjon for det de gjør. (Informant 41).*

Bigtechaktører skiller seg fra mindre fintechene i deres ressurser, kompetanse og allerede eksisterende brukerbase. En kan derfor vurdere at bigtechs på lang sikt, vil ha størst innvirkning på betalingsformidlingen. Norske banker har allerede inngått samarbeid med aktører som Google og Apple, tilknyttet deres betalingsløsninger (Finanstilsynet, 2019, s. 15). Løsningene implementert av aktørene er som indikert i sitatet ovenfor utenfor konsesjon, dette er derimot en introduksjon av bigtechs til norsk betalingsformidling. En potensiell risiko er konsentrasjon av brukere hos nye bigtechaktører. Problematikken knyttet til dette er ikke bare at norske brukere potensielt blir avhengige av utenlandske tilbydere av betalingstjenester.

Betalingstjenester vil videre ikke kunne kontrolleres i like stor grad av norske myndigheter og banker i tilfeller ved bortfall av tjenestene.

> *Det er jo et scenario at for eksempel Amazon lager et system og mobiltjeneste som har en brukeropplevelse som gjør at alle tar i bruk det å bare slutter folk å bruke mobilbanken til sin egen bank fordi de får så mye mer hos Amazon. Da kan vi komme dit hvor vi får et smalere spekter og ikke et bredere et. Slik at man i Norge risikerer å være helt avhengig av at løsningene til Amazon fungerer. (Informant 21).*

Ved slike tilfeller vil det foreligge både styringsproblem for myndigheter og banker og en konsentrasjonsrisiko knyttet kundene som benyttet tjenester av bigtechaktøren. Samtidig kan store bigtechaktører svekke det norske betalingssystemet ved at de trekker større volum av norske transaksjoner. I et slikt scenario kan det tenkes at den norske infrastrukturen vil kunne til dels avvikles.

> *Det kan jo hende at disse tredjepartsleverandørene kan gjøre mye av denne avregningen selv, sånn at behovet for NICS i fremtiden bli mindre. (Informant 22).*

Scenarioet er dog lite plausibelt i nær fremtid ettersom bankene sitter på de underliggende betalingsinstrumentene og kontoaksess nødvendig for transaksjoner (Norges Bank, 2019, s. 11). Samtidig banker er de eneste som får delta i interbankclearing- og oppgjøret (Bits AS, 2018c, s. 2; Bits AS, 2018l, s. 1). En kan derimot se trekk som indikerer at flere større teknologiaktører ønsker å lansere egne virtuelle valutaer, e-penger, som de kan utstede til brukerne (Norges Bank, 2019, s. 11). Dette kan på sikt presentere en trussel mot avregningsentralen og NBO, en slik utvikling kan også være problematisk med tanke på sårbarhet. I et slikt tilfelle vil avregning og oppgjør, ved stor oppslutning rundt løsning, knyttet til betalinger gjort av norske brukere i stor grad bli gjort av et utenlandsk foretak. I slike tilfeller vil det være vanskelig for norske tilsynsmyndigheter å kunne vurdere hvordan dette foregår. Samtidig vil det være problematisk å kunne pålegge en slik aktør å følge regler og reguleringer påsett i Norge. På en annen side så må bigtechs først få konsesjon til å drive som et e-pengeforetak før de kan påbegynne noe slikt, her kan tilsynsmyndigheter pålegge aktøren en rekke krav til tilsyn og sikkerhet jf. Finansforetaksloven (2015, § 3-1).

Et videre aspekt knyttet til sårbarhet ved inntoget av bigtechs er informasjonshåndtering. Bruk av dataen større blant teknologiselskapene kan være problematisk, herunder kan en trekke frem hendelsen med Facebook og Cambridge Analytica (Elster, 2018).

> *Det er jo en fare, ved at de ikke følger personverndirektivet til punkt og prikke. Kundene blir utnytta på en annen måte, for bankene har vært utrolig flinke på å ikke bruke kundedataene til markedsføring og*

lignende. For de har holdt seg innenfor det de normalt skal gjøre og har gjort avtale med kundene om. (Informant 21).

Informasjonssikkerhet og personvern er noe som kan potensielt bli en sårbarhet hos slike aktører. Slike aktører vil sitte på vesentlige mengder data om brukerne, gjennom sitt opprinnelige virke med også transaksjonsdata som kan benyttes til markedsføring og lignende. Hvorvidt dette er et problem for sårbarheten i betalingsformidlingen og samfunnssikkerheten er noe som må diskuteres. En kan dog poengtere hvordan dette kan skape problemer for brukeren, da påvirkning av kunden og kundeatferd kan påvirkes på lik linje som ved Cambridge Analytica-saken.

Men vi er litt bekymra for at de store internasjonale ikke er så nøye på det og heller bruker transaksjonsdata og kanskje selger de og sånt. Hvert fall mer bekymra for dataene til kundene enn akkurat det som går på betaling. (Informant 21).

Samtidig foreligger det restriksjoner på hvordan persondata skal håndteres, internt i EØS foreligger GDPR, også kalt personverndirektivet som begrenser omfattende bruk av persondata. For foretak utenfor EØS må de sertifiseres for bruk av persondata i henhold til Privacy Shield (Datatilsynet, 2018b).

Kombinasjonen av at nye større aktører kan komme til å håndtere mye informasjon om brukerne kombinert, med at potensielt mange velger å benytte seg av bigtechs for betalingstjeneste, kan medføre som poengtert, konsentrasjonsrisiko. Bigtechenes konsentrasjon av informasjon kan gjøre dem til attraktive for målrettede angrep (Norges Bank, 2018a, s. 4). Den potensielle konsentrasjonen av brukere og informasjon om brukere kan være en potensiell fremtidig sårbarhet, særlig i tilfeller ved målrettede angrep mot slike aktører. En kan derfor vurdere hvorvidt slike aktører kan svekke sårbarheten for betalingsformidling. Samtidig må det poengteres at brukerne allerede gjerne allerede har løsninger knyttet til eksisterende norske banker og ergo norsk betalingsformidling og –infrastruktur.

Outsourcing, tjenesteutvikling på bekostning av styring?

Konseptet om å sette ut tjenester er som fenomen ikke nytt, slike strategiske beslutninger har foretak benyttet seg av i lengre tid (Lonsdale & Cox, 2000, s. 447). Potensielle problem og sårbarheter er dog vedvarende, endrede og nye. Et problem tilknyttet styringsdimensjonen er å avdekke kritiske deler i verdikjeden. Uttømmende outsourcing, kan gjøre verdikjeden uoversiktlig, ergo vi det være problemer med å kartlegge verdikjeden (NOU 2015:13, s. 176; NOU 2018:14, s. 20).

Fordi det man ser at for å levere en tjeneste kan det være behov for å flere sentrale leverandører til det, noen har typisk en stor leverandør på det vi kaller stormaskin eller basisløsningene. Og så er det noen som har leverandør på nettbanken sin. Er det noe som er feil, så trenger ikke nødvendigvis den feilen være 100% på den ene eller andre siden, det kan være samspillet mellom de. Og det å da ha på plass rutiner for effektiv problemløsing er viktig, uavhengig hvor mange leverandører man har. (Informant 41).

Verdikjedene som underbygger tjenesteleveransen til foretakene er typisk ikke bestående av en underliggende funksjon, men gjerne flere. En kan derfor forvente at i en verdikjede så vil det gjerne inngår flere tjenester, funksjoner og oppgaver som underbygger tjenesteleveransen. Dette kan resultere i økt kompleksitet og en kompleks leverandørkjede. I tjenesteleveransen til bankene foreligger det indisier som peker på økende kompleksiteten i verdikjedene, særlig tilknyttet IT-leveransen (Finanstilsynet, 2019, s. 58). Kompleksiteten er samtidig ventet å øke som en følge av skytjenester stadig mer flittig benyttes av foretakene. Herunder vil større internasjonale aktører som Amazon, Microsoft og Google være sentrale (ibid., s. 32).

Avslutningsvis er det av flere poengtert problemstilling knyttet til outsourcing med fremtidige konsekvenser, omfanget er dog noe uvisst. Bortfall av kompetanse er noe som foretakene kan oppleve ved outsourcing. Allerede foreligger det indikasjoner som tyder på at problemet forekommer (Finanstilsynet, 2019, s. 39). Dette kan være problematisk ved tilfeller hvor en ser seg nødt til å insource tjenester og funksjoner som tidligere er vært satt ut. Problemer ved å drifte og utvikle tjenesten vil påvirke funksjonaliteten og sikkerheten til tjenesten (ibid.).

Det kan jo være en utfordring i norsk finansnæring på sikt, om man plutselig er i en opplever en situasjon hvor man er nødt til å insource sånne aktiviteter igjen så har man ikke ressurser til å gjøre det. (Informant 11).

På lengre sikt kan en forestille seg scenarier hvor norske finansinstitusjoner i ytterligere grad må insource og ta over aktiviteter. Sentralt i slike situasjoner er kunnskapsdimensjonen, i tilfeller hvor tjenester i lengre tid er satt ut til eksterne leverandører kan en forvente en forvitring av kunnskap til funksjonen som nå insources. Kunnskapsmangler kan derfor potensielt i fremtiden være opphav til vesentlige sårbarheter i norsk betalingsformidling.

Vi kan ikke sette bort hele områder uten at man da i så fall har avtaler om at det i langlang fremtid skal håndteres av den andre parten. Vi passer på at det er kompetanse i organisasjonen sånn at det alltid har med noen som kan ta tilbake det som gjøres, og forvalte og drifte det i organisasjonen. Det er en av utfordringene ved outsourcing som vi har måttet lære av over tid. Så vi passer alltid på at det er miks, både at det er ressurser i organisasjonen og hos de vi outsourcer til, som kjenner og jobber med oppgaven sånn at vi får ivaretatt kompetansen i egen organisasjon. (Informant 21).

Outsourcing må i tråd med utdraget, ikke gå på bekostning av fremtidig eller eksisterende kompetanse i foretaket. Kunnskapen ved outsourcing kan bortfalle om det er problemer knyttet til kunnskapsoverføring (Gottschalk, 2013, s. 26). Problemer med kunnskapsoverførsel kan også gå andre veien, hvor foretaket ikke i tilstrekkelig grad formidler kunnskap om drift og utviklingen av funksjonen til underleverandør.

Oppsummering forskningsspørsmål 2

Tabellen summerer opp de mest fremtredende funnene knyttet til forskningsspørsmål 2.

Tabell 7 Oppsummering funn FS2

Oppsummering funn FS2
- Det finansielle systemet i Norge er på generelt grunnlag ansett robust - Fremtiden presenter dog stor usikkerhet til utformingen av betalingsformidlingen, særlig på lengre sikt.
Eksisterende sårbarheter
- Konsentrasjon rundt få driftsoperatører av bankenes tjenester flere av FOIene, deriblant NICS, ansees som en risiko og potensiell sårbarhet. - Enkelte FOIer tjener flere formål, BankID har i tillegg opplevd flere tilfeller som har resultert i bortfall - Pr. i dag er det ingen direkte uavhengig alternativ løsning fra eksisterende elektroniske betalingsløsninger.
Trusselbilde
- Trusselbilde er stadig i endring. - Infrastruktur og de som arbeider rundt infrastruktur oppfattes som mulig mål for målrettede angrep.
Beredskap
- Det foreligger flere beredskapsløsninger tilknyttet forskjellige funksjoner sentralt for betalingsformidlingen. - Beredskapen i elektroniske betalingstjenester oppfattes ikke av sentrale myndigheter som tilstrekkelig uavhengig hverandre. Derfor er kontantberedskap introdusert. - Finans Norge oppfatter kontantberedskap som lite samfunnsøkonomisk. - NordiskFinansCERT opererer som en overnasjonal organisasjon som utøver arbeid knyttet til sikkerhet, risiko og beredskap i cyberdomenet.
Potensielle nye sårbarheter
- Stor endringstakt representerer i seg selv en risiko for betalingsformidlingen. - Nye aktører presenterer gjennom PSD2 og open banking økt angerepsflate mot bankene og øker kompleksiteten i systemet. - Bigtechs kan på lengre sikt utfordre norsk betalingsformidling. - Interbanksystemet forventes å være uberørt av nye aktørers inntog, smitteeffekt fra hendelser hos bankene er dog fortsatt en potensiell trussel. - Kompetanse- og ressursmangel påpekes som varseltegn ved nye aktører. - Outsourcing utfordrer foretakenes evne til å styre verdikjedene, gjerne tilknyttet manglende bestiller-kompetanse og ergo manglende avtalebeskrivelser. - Outsourcing medfører økt kompleksitet i verdikjeden for ulike tjenester som igjen medfører økt risiko og potensielt økt sårbarhet. - Bortfall kan ramme foretak som en konsekvens av outsourcing.

6. Drøfting

Kapittel 5 har belyst FS1 og FS2, dette kapittelet vil ved bruk av teori vurdere hvorvidt flere aktører vil påvirke samfunnssikkerheten ved besvarelse av FS3. I kapittel 6.2 vil problemstillingen besvares.

6.1 Endringer i betalingsformidlingen og dets konsekvenser for samfunnssikkerheten

Først er det hensiktsmessig å utlede forskningsspørsmål 3 som er grunnlaget for kapittelet.

Hvilke konsekvenser kan et bredere spekter av aktører ha for betalingsformidlingen i Norge?

Kapittelet begynner først med å se hvordan endringer i systemet, herunder inntoget av nye aktører, vil innvirke på betalingsformidlingen. Dernest trekkes det tråder til hvorvidt nye aktører kan medvirke i oppbygning av latente forhold og aktive feil i systemet. Videre sees det på hvordan barrierer i betalingsformidlingen har innvirkning på sikkerheten. Prinsippene for samfunnssikkerhet og beredskapsarbeid drøftes siden, og det vurderes hvordan nye aktører utfordrer eksisterende aktørers etterlevelse av prinsippene.

6.1.1 Systemets generelle utvikling

Normal Accidents, en iboende karakteristikk ved betalingsformidling?

Charles Perrow foreskriver hvordan system med visse trekk kan ha iboende systemulykkepotensial, herunder vil et systems forutsetninger for styring og ulykker bero på hvordan systemet kan karakteriseres i henhold til dimensjonene koplinger og interaksjoner (Perrow, 1999, s. 5).

Perrow (1999) foreskriver koplinger som en måte å vurdere hvordan et system er bygget opp. Det norske betalingssystemet er bygget opp rundt felles løsninger og er følgelig avhengig av FOIer og særlig avregning i NICS og oppgjør i NBO (Norges Bank, 2018a, s. 20). Avregningen mellom norske banker skjer fem ganger daglig før det sendes til oppgjør i NBO (Norges Bank, 2018b, s. 68). Her vil en ha et system som avhenger av tidsavhengige prosesser, noe som er et trekk ved tette koplinger. I systemer karakterisert av tette koplinger vil forsinkelse i et ledd forsinke det neste leddet i prosessen (Perrow, 1999, s. 93). En kan her se til hendelsen som omtalt, hvor avregningen i 2018 stanset grunnet avvik i flere timer, noe som forsinket betalingsformidlingen inneværende dag (Bits AS, 2018a, s. 3). Sentraliteten til NBO og NICS kan neppe erstattes på kort tid av en alternativ løsning som vil gi tilstrekkelig resultat, noe som gjør at utskiftninger av komponenter i produksjonssløyfen er vanskelig. Det jobbes dog med en lansering av NICS Real som vil fungere som et faktisk RTGS-

avregningssystem med ingen form for likviditetsrisiko hos bankene (Bits AS, 2018a, s. 22). Avvik i NICS og NBO vil følgelig få vesentlige konsekvenser for resten av «produksjonen» som er transaksjoner i det norske samfunnet (ibid., s. 3, 16). Interbanksystemet er derfor preget av det Perrow (1999, s. 94) betegner som tette koplinger.

Det foreligger flere ulike måter å initiere transaksjoner, noe som indikerer at det foreligger ulike produksjonsmåter i systemet (Perrow, 1999, s. 94). Systemet for betalinger kan til tross for dette beskrives som tett koplet. Betalingstjenestene er knyttet til ulike funksjoner, som f.eks. at kortbetalinger er knyttet til EFTPOS-transaksjoner, regningsbetaling kan gjøres ved hjelp av eFaktura eller AvtaleGiro og Straksbetalinger kan benyttes til P2P-betalinger. Ergo hver form for betaling vil skape et ulikt «produkt» og derfor ikke nødvendigvis inngå i samme produksjonssystem (NOU 2015:13, s. 169). Samtidig vil ulike betalingstjenester benytte til dels ulike meldingsformat når de sendes inn til avregning, noe som igjen gjør prosessen tettere koplet da de spesifikke meldingsstandardene er knyttet til transaksjonsformen (Bits AS, ingen dato(e)). En kan vurdere hvordan denne oppsplittede funksjonaliteten på tjenestene vil endres ved nye tjenestetilbydere og innførselen av ende-til-ende meldingsstandarden ISO 20022 (Bits AS, ingen dato(f)).

Betalingstjenestene i seg selv er tidssensitive og det foreligger et bestemt mønster for hvordan gjennomføring av transaksjonen. Dette gjelder særlig ved bruk av bankkort, herunder BankAxept, hvor transaksjonsløypa illustrert i figur 5 viser transaksjonsflyten. Ved EFTPOS-transaksjoner så foreligger det gang i transaksjonsløypa som må ligge til grunn for at transaksjonen, en debetbetaling, kan gjennomføres (ibid., s. 70-71). Ved debetbetalinger knyttet til BankAxept har derfor også en gitt «produksjonsmåte» som indikerer tette koplinger (Perrow, 1999, s. 94). De alternative måtene å initiere kortbetalinger på, da tenkt gjennom kredittkort eller faktureringskort benytter alternative transaksjonssløyfer. En kan derfor diskutere hvorvidt norsk betalingsformidling virkelig er tett koplet sammen. Sentralt i en slik diskusjon er at slike betalinger kun indirekte er knyttet til norsk betalingsformidling og i så måte ikke nødvendigvis inngår i systemet for norske kortbetalinger.

Inntoget av nye aktører, særlig knyttet til betalingsinitiering virker ikke å gjøre systemet ytterligere tett koplet. En slik vurdering legger til grunn tilgangen nye tredjepartsaktører får gjennom PSD2 og bilaterale samarbeid, herunder vil de tilknyttes bankene gjennom et dedikert grensesnitt (Norges Bank, 2017, s. 9). Nye betalingstjenester vil i stor bygge på kontoinformasjon, transaksjonsdata og personopplysninger (Norges Bank, 2019, s. 10). Tjenestene som allerede er introdusert av bigtechs belager seg på betalingsinstrumenter som

utstedes og betjenes av bankene (ibid., s. 4). Nye aktører introduserer ikke nye betalingsinstrument som det må tas høyde for i betalingsformidlingen. Outsourcing kan dog til en viss grad innvirke på koplinger i betalingssystemet, men effekten er forventet og også være begrenset. Mye grunnet at outsourcing nå og fremtidig i all hovedsak omhandler drift og utvikling av tjenester, noe som ikke nødvendigvis direkte berører foretakenes betalingstjenester.

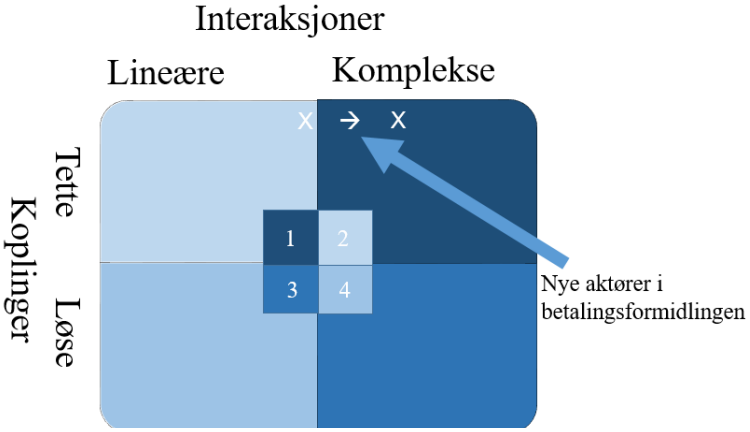
Den andre dimensjonen Perrow (1999, s. 72) karakteriserer system ut ifra er samspillet mellom komponentene. Det skilles her mellom lineære og komplekse interaksjoner. Lineære interaksjoner er gjerne tilknyttet kjente produksjonssløyfer, segregerte prosesser som etterfølger hverandre og komponentene som inngår i systemet tjener en funksjon (ibid., s. 75). Det er trekk ved betalingsformidlingen i Norge som indikerer å inneha enkelte av karakteristikkene. Transaksjonssløyfen for betalinger er godt kjent for deltakerne i systemet, bankene, og dette gjør at en kan enkelt forutse hvordan systemet interagerer med ets deltakere og komponenter. Samtidig er aktørbildet av de som er involvert i interbanktransaksjoner begrenset, herunder må foretak som ønsker deltakelse ha konsesjon for bankvirksomhet, og gjennom medlemskap i FNO og eller særskilt tillatelse fra Bits AS for kunne delta (Bits AS, 2018c). En slik forutsigbarhet taler for at systemet har lineære interaksjoner, samtidig foreligger det indikasjoner på at prosessene i systemet er tilstrekkelig segregert. Eksempelvis kan en vise til at på bakgrunn av transaksjonsinstrument som benyttes vil det benyttes en meldingsstandard, avhengig av betalingsmåte, for å sende interbanktransaksjoner til NICS (Bits AS, ingen dato(e)). Implementering av ende-til-ende meldingsstandarden ISO 20022 er dog noe som kan utfordre en slik segregering (Bits AS, ingen dato(f)). Standarden kan brukes til flere formål, ergo så vil den kunne medføre økt effektivitet (Bits AS, 2016b, s. 10). En vil med dette ha en meldingsstandard som tjenere flere formål, noe som kan medføre komplekse interaksjoner.

Noe som taler imot at systemet er preget av lineære interaksjoner er BankID som opererer som autentisering- og verifiseringstjeneste for flere funksjoner enn kun nettbank og netthandel (NOU 2015:13, s. 170). Herunder tjener funksjonen multiple formål og interagerer med ulike komponenter innad i systemet, samt andre system. En annen FOI som tjener multiple formål er autoriseringstjenesten BALUTUS 2.0. Tjenestens funksjon omhandler autorisering så FOIet opererer på flere nivå i verdikjeden for betalingsformidling (Bits AS, ingen dato(d)). En slik funksjonalitet kan indikere at BALTUS 2.0 interagerer med komponenter som ellers ville

vært segregerte. Et videre aspekt som peker på at systemet har, og ventet å øke, komplekse interaksjoner og er en tendensene knyttet til underleverandører og leverandørstyring.

Foretak i norsk betalingsformidling benytter seg flittig av outsourcing for leveranse av sine tjenester, dette medfører fragmentering i verdikjeden for tjenesteleveranse (NOU 2015:13, s. 170). Særlig kan outsourcing av drift til samme leverandører (Norges Bank, 2018a, s. 7; NOU 2015:13, s. 175) medføre både en konsentrasjonsrisiko men også interaksjon mellom funksjonene som gjennom driftsoperatøren. Samtidig kan en snakke om nærhet, som også er kjennetegn ved komplekse interaksjoner (Perrow, 1999, s. 75-76). Nærhet mellom komponenter ser en særlig knyttet til en av driftslokasjonene for betalingsformidlingen. Den ene driftslokasjonen til NICS er samlokalisert med systemene til en rekke andre foretak sentrale i norsk betalingsformidling (Norges Bank, 2018a, s. 28). En kan potensielt snakke om skjulte interaksjoner mellom de ulike komponentene som driftes av de større aktørene. Slike interaksjoner vil dog være vanskelig å avdekke, da de følgelig er skjulte og ikke kjente, men kan likeverdig prege systemene (Perrow, 1999, s. 78-79). Samtidig vil nye aktører i verdikjeden for betalinger, noe som medfører flere interaksjoner mellom de ulike delene som inngår i verdikjeden. Interaksjonene kan forventes å være lineære forutsatt: at aktørene introduseres gjennom PSD2-grensesnitt; et open banking-grensesnitt som er utformet tilstrekkelig, gjerne i henhold til en standard jf. European Central Bank (2019, s. 1-2); eller gjennom outsourcing hvor det foreligger en tilstrekkelig avtale. Til tross for dette kan både komplekse og skjulte interaksjoner forekomme, dette er dog vanskelig å predikere (Perrow, 1999, s. 78-79), men står heller som et tankekors.

Betalingsformidling trender derfor til å bevege seg i modellen presentert av Perrow (1999, s. 97) mot karakteristikker som betegner et system med både tette koplinger og komplekse interaksjoner. Kompleksiteten er ventet å øke grunnet uoversiktligheten i verdikjeden til bankene. Særlig outsourcing kan bidra til dette (Gottschalk, 2013, s. 17; NOU 2018:14, s. 20). I en slik logikk vil en derfor kunne forvente at en en *Normal Accident* vil inntreffe som et plausibelt utfall av økt kompleksitet i interaksjonene.



Figur 13, betalingsformidling ved endringer, i lys av Perrow (1999, s. 97)

Selv om systemet vurderes til å ha flere komplekse interaksjoner og ergo være mer utsatt for systemulykker er ikke dette en egenskap som nødvendigvis er iboende. Perrow poengterer hvordan verdipapir og valutautvekslinger i finansmarkedet bidrar til økt omfang av komplekse og tette koplinger i finansmarkedet (Perrow, 1999, s. 385). Det kan trekkes paralleller til betalingsformidlingen og at nye aktører og uoversiktlige verdikjeden øker kompleksitet og at systemet for betalingsformidling iboende er tett koplet. Herunder vil en kunne se at systemulykker vil være plausibelt. Om en ser til den lignende diskusjonen omkring finansmarkedet, indikeres det at økt kompleksitet i interaksjonene og tette koplinger er egenskaper som aktører har tilført systemet, ikke iboende egenskaper for «produksjon». Ergo, systemulykker er ikke en iboende egenskap ved systemet (ibid., s. 387). Det kan trekkes paralleller til norsk betalingsformidling, utviklingen og digitalisering av betalingssystemet er i stor grad grunnet aktørenes ønske om effektivisering av systemet jf. kapittel 2. Videre innovasjoner skyldes igjen et ønske om tilpasning til internasjonale trender, forbedringer av eksisterende system og igjen effektivisering. I dag er rasjonale bak PSD2 et ønske om bedre tjenesteutvalg for kundene og utvikling av sikre effektive løsninger (Norges Bank, 2017, s. 9). Open banking-plattformen bygger på en lignende logikk, men med initiativ fra bankene og tredjepartstilbydere. Outsourcing kan som open banking, sees som en strategisk beslutning fra bankenes side om effektivisering og innovasjon av tjenester. Herunder er systemegenskapene tillagt, i dag og fremtidig, noe som ved finansmarkedet indikerer at egenskapene ikke er iboende (Perrow, 1999, s. 387). Systemet for betalingsformidling kan ergo føres tilbake til simplere omstendigheter hvor kontanter er det ledende betalingsinstrumentet. Kontanter er fortsatt tvungne betalingsmidler i henhold til Finansavtaleloven (1999, § 38-3).

Organisatoriske ulykker i betalingsformidling

Reason (1997) presenterer som Perrow (1999) en teori knyttet til systemulykker, Reason har dog en annen tilnærming til hvordan systemulykker kan oppstå. Sentralt i Reason (1997) sin teori om organisatoriske ulykker er aktive feil og latente forhold, disse faktorene greiner mangt og er sentrale i hans forklaring på fremkomsten av ulykker. Aktive feil er som poengtert av Reason (1997) handlinger som begås av operatører i den skarpe enden av operasjonen. Hvorvidt slike hendelser vil oppstå mer frekvent og hvordan slike hendelser oppstår ved inntoget av nye aktører er vanskelig å vurdere. En kan imidlertid i større grad vurdere hvorvidt inntoget av nye aktører kan medføre at latente betingelser kan bidra til økt risiko og sårbarhet i betalingsformidlingen.

Introduksjon av fintechs og bigtechs til betalingsformidling gjennom open banking og eller PSD2 vil i all hovedsak bygge på den eksisterende verdikjeden da deres tjenester vil bygges opp rundt bankene (Norges Bank, 2018a, s. 12), ved tilgang på konto- og transaksjonsinformasjon gjennom et standardisert grensesnitt (PSD2, 2015, Artikkel 66 & Artikkel 67). Verdikjeden vil derfor bli lengre, dette i seg selv vil resultere i økt eksponering og økt risiko som en konsekvens av at flere aktører inngår i økosystemet for betalinger.

> *Det er ofte spekulert i at lengre verdikjeder og nye aktører skaper ny sårbarhet, min holdning er at så lenge de nye aktørene er regulert så skaper de ikke en annen sårbarhet enn at det er en annen aktør inn i systemet. (Informant 41).*

En kan vurdere hvorvidt aktørenes deltakelse i verdikjeden for betalingsformidlingen vil kunne bygge opp latente forhold som er av relevans for foretakenes andre tjenester. En kan grunnet begrensninger knyttet til tilgangen gjennom grensesnittene i PSD2 forvente at latente forhold og potensielle aktive feil som gjøres ved tredjepartsaktøren vil kun påvirke aktøren og dets brukere. Ergo presenterer ikke inntog av tredjepartsleverandører gjennom PSD2 vesentlige konsekvenser for norsk betalingsformidling.

> *Det PSD2 var skrevet og ment for å gjøre var å lage et sikrere system men samtidig å åpne for konkurranse ved å fjerne en del av de barrierene som bankene har bygget rundt sine tjenester. For å gi bedre tjenester og vilkår til brukerne, det var det PSD2 i utgangspunktet var ment til å være. Det det nå har blitt gjennom intens lobbyering fra de mer etablerte aktørene, er en veldig strupet og begrenset effekt. (Informant 31).*

Det kan derimot oppstå latente betingelser, som kan inkuberes i tredjepartsleverandørenes tjenester og virke. Som ved aktive feil kan utløse hendelser hos tredjepartsleverandøren som hindrer aktøren og dets brukere i å utføre tjenester og ens funksjon (Reason, 1997, s. 10). Hvorvidt en kan vurdere dette som sannsynlig er vanskelig, men gjennom tilsyn og at aktører trenger konsesjon (Finanstilsynet, 2019, s. 16) kan en forvente at det foreligger en god praksis knyttet til sikkerhet og risikostyring hos aktørene. Ved bortfall av en tredjepartsleverandørs tjenester vil det kunne være problematisk å initiere eller gjennomføre tjenester i nevnte plattform. Ergo vil hendelser kunne oppstå i systemene for tredjepartsleverandører, men en kan ikke betegne dette som organisatoriske ulykker pr. definisjon grunnet dets manglende effekt på betalingsformidlingen ellers.

Open banking er ikke regulert på lik linje med PSD2. Avtaleforholdet mellom foretak og tredjepartsleverandør er her grunnlag for introduksjon (Evry AS, 2017, s. 24). Vurderinger omkring latente betingelser og hvordan dette kan oppstå kan ventes å ha lignende trekk som

ved PSD2. Forskjeller kan dog legges til at grensesnittet kan være designet annerledes (Finanstilsynet, 2019, s. 15), kaskadeeffekter kan som en følge av dette være større. Informant 41 poengterer at sikring må være fokus for aktørene ved samarbeid.

(..) Tilgangen basert på open banking er ikke regulert og krever mye bedre avtale og sikring mellom aktørene og ikke minst i forhold til brukerne. (Informant 41).

Herunder blir det bilaterale avtaleforholdet og utviklingen av tilhørende grensesnitt sentralt for sikkerheten i løsningen. Informant 21 trekker nettopp denne problematikken frem

Så jeg tenker nok at open banking kan utfordre sikkerheten hvis ikke bankene er veldig bevist på det. (Informant 21).

En utfordring for bankene er å definere omfanget på grensesnittet og ergo tilgangen som gis til tredjeparten. Såfremt tilgangen gjennom grensesnittet ikke gir tilgang til tjenester utover PSD2 er det dog ikke å forvente at aktørene vil innvirke på foretakets generelle sikkerhet, dette er foreskrevet av Finanstilsynet (2019, s. 49). En kan derimot vurdere at det foreligger tilfeller hvor bankene og tredjepartsleverandørene ikke gjennomfører hensiktsmessige vurderinger og derfor kan latente forhold i større grad bygges opp mellom partene. Ringvirkningene for bankene kan også bli mer betydelig i tilfeller grensesnittet ikke er designet med tilstrekkelig sikkerhet.

Outsourcing av aktiviteter, funksjoner og tjenester påvirker verdikjeden annerledes, ved outsourcing er det funksjoner i den eksisterende verdikjeden som overtas av eksterne aktører (Power et al., 2006, s. 3). Her vil «nye aktører» introduseres til betalingsformidling mer direkte relatert til bankenes evne til å levere funksjoner. Ergo mer direkte innvirkning på bankenes betalingstjenester, da underleverandøren overtar tjenester tidligere driftet av foretaket (ibid., s. 4). Ved underleverandørers aktive innvirkning på leveransen av funksjoner blir aktive feil og latente betingelser mer problematisk. Latente betingelser kan oppstå med bakgrunn i strategiske valg (Reason, 1997, s. 10). Outsourcing er i seg selv et strategisk valg som faller innunder et foretaks veivalg knyttet til drift, utvikling og støttefunksjoner av sine tjenester (Gottschalk, 2013, s. 24-25). En kan derfor vurdere hvordan videre og utstrakt utkontraktering av funksjoner kompliserer verdikjedene. Konsekvenser av outsourcing kan medføre oppbygging av latente betingelser og siden aktive feil, det trekkes paralleller til Reason (1997, s. 46) og problematisering rundt automatisering. Hvor automatisering kan skape problemer som økt kompleksitet, dårligere informasjonsflyt og bortfall av kompetanse i foretaket. Problemene er også gjeldende ved outsourcing, ved at foretakenes verdikjeder

stadig blir mer kompleks (NOU 2015:13, s. 176; NOU 2018:14, s. 20). Økt kompleksitet vil kunne skjule forhold av interesse for foretakene og sikkerhet knyttet til verdikjeden og ergo funksjonen den tjener.

Gottschalk (2013, s. 17) har også identifisert at kompleksiteten kan medføre at bankenes aktiviteter ikke lenger kan sees i en lineær og etterfølgende verdikjede, noe som gjør styring av verdikjeden vanskelig. Et ytterligere problem ved uoverskuelighet i verdikjeden er problematikk i å identifisere kritiske komponenter. Problematikken rundt manglende kjennskap til egen verdikjede er noe Finanstilsynet (2018, s. 20) har trukket frem. Her poengteres at bankene ikke i tilstrekkelig grad inkluderer slike vurderinger i sine interne risikoanalyser. Manglende innsikt i ens verdikjede kan medføre at banken ikke har oversikt over frembringelse av latente forhold, som medfører at systemet svekkes uten at foretaket er klar over det (Reason, 1997, s. 10). En kan i så måte vurdere hvorvidt outsourcing kan skape problemer og potensiale for organisatoriske ulykker i betalingsformidlingen. Samtidig kan det ikke underdrives at outsourcing er underlagt visse lovbestemmelser som i viss grad dikterer hva som kan outsources. Finanstilsynet har også hjemmel i Finanstilsynsloven (1956) § 4 c., til å stoppe eller påse at outsourcing som innebærer at et foretak utsetter tjenester som kan medføre manglende sikkerhet eller innvirker på deres konsesjonsbelagte tjenester insources. På bakgrunn av Finanstilsynets hjemmel og lovfestede pålegg til outsourcing, kan en ikke forvente at latente forhold lengre ned i verdikjeden noe som nødvendigvis direkte vil prege betalingsformidlingen.

Bortfall av kompetanse ved outsourcing også et aspekt som kan skape latente forhold. Her overtar nye aktører tjenester og aktiviteter, potensielt også kunnskap, tidligere holdt internt.

> *Det kan jo være en utfordring i norsk finansnæring på sikt, om man plutselig er i en opplever en situasjon hvor man er nødt til å insource sånne aktiviteter igjen så har man ikke ressurser til å gjøre det. (Informant 11).*

Problematikken belyst av informanten er allerede noe som fremgår i norsk betalingsformidling. Flere foretak som nå insourcer aktiviteter og tjenester har opplevd problemer med drift og håndtering av tjenesten (Finanstilsynet, 2019, s. 39). Latente forhold, kompetansebortfall i dette tilfellet, legger grunnlaget for aktive feil, les: problemer med drift av tjenesten som er insourcet. Årsaken til kompetansebortfall kan tillegges manglende kunnskapsoverføring mellom avtalepartene. Kunnskapsoverføring er tidligere poengtert som en problematikk knyttet til outsourcing (Gottschalk, 2013, s. 26). Her stilles det krav til foretakene om å fatte tiltak for å begrense omfanget av kompetansebortfall.

Så vi passer alltid på at det er miks, både at det er ressurser i organisasjonen og hos de vi outsourcer til, som kjenner og jobber med oppgaven sånn at vi får ivaretatt kompetansen i egen organisasjon. (Informant 21).

Ettersom de konsesjonsbelagte funksjonene banken tjener, eller oppgaver sentralt for å betjene disse ikke kan utkontrakteres i henhold til Finanstilsynsloven (1956) § 4 c., kan en vurdere hvorvidt konsekvensene knyttet til outsourcing innvirker på systemets sikkerhet. Og herunder samfunnssikkerheten.

Latente forhold kan altså bygges opp i betalingsformidlingen gjennom introduksjon av nye aktører. Samtidig kan det poengteres at det forventede potensialet til nye aktørers innvirkning og latente forhold mellom nye og eksisterende aktører forventes til å ikke å ha et reelt potensialet for organisatoriske ulykker. Bortfall av kompetanse, styringsproblemer og dårlig definerte grensesnitt kan dog introdusere latente forhold av betydning og som kan medføre vesentlige konsekvenser.

6.1.2 Barrierer, begrensende for nye aktørers innvirkning på betalingsformidling?

Av foregående kapittel er det klart at nye aktører *kan* innvirke på sikkerheten i betalingsformidlingen. Nå skal det derimot vurderes hvilken tilgang nye aktører kan ventes å få til det eksisterende betalingssystemet.

Interbanksystemet

Nye aktører tilgang til interbanksystemet og de felles betalingstjenestene avgjøres av lover, forskrifter og regler fastsatt av myndigheter og FNO. Herunder blir barrierene, jf. Hollnagel (2004) sin forståelse lagt til grunn. Hollnagel (2004, s. 68) beskriver barrierer som *en hindring som kan innvirke på hvorvidt en uønsket hendelse inntreffer og konsekvensene ved uønskede hendelser*.

Hvilke aktører som får tilby betalings-, konto- og banktjenester avgjøres av et system som er gjennomregulert og i betydelig grad omfattet av regler. Reguleringene omfatter blant annet Betalingssystemloven (1999); Finansavtaleloven (1999); Finansforetaksforskriften (2017); Finansforetaksloven (2015); Finanstilsynsloven (1956); PSD2 (2015); og «Blåboka» (Bits AS, 2018m). Disse legger føringer for atferd og krav stilt til foretakene som deltar i betalingsformidlingen. En kan forvente at slike reguleringer samt tilsynsmyndighetene som ser til at dette etterleves (Norges Bank, 2018a, s. 3; NOU 2015:13, s. 169), vil operere som barrierer i henhold til definisjonen som foreligger fra Hollnagel (2004, s. 68). Herunder vil reguleringene opptre som barrierer i lys av betegnelsen myke barrierer, hvor regler er inkludert (Reason, 1997, s. 8). Omfatningen av lovene og forskriftene og at tjenestene knyttet

til betalingsformidling i stor grad er underlagt konsesjon indikerer myke barrierer. Slike barrierer kan sies å være en blanding av passive og aktive barrierer, hvor lover og reguleringer ikke krever aktivering fra eksternt hold og i så måte er passive (Aven et al., 2004, s. 122; Kjellén, 2000, s. 86). På en annen side krever lover og reguleringer oppfølging fra relevante myndigheter for å håndheves, samt vurdere og utgi konsesjon til tjenesten noe som peker på aktive barrierer (Aven et al., 2004, s. 122). Samtidig foreligger det indisier som tilsier at systemet har en rekke logiske barrierer. Grunnet manglende tilgang til, og derigjennom innsikt i dokumentasjonen knyttet til dette gjør det vanskelig å vurdere.

Knyttet til selvreguleringsregimet og tilgang til bankenes FOIer og felles betalingstjenester foreligger det også bruk av reguleringer. Herunder foreligger det en adgangsbegrensning som har både hjemmel i lov og tilknyttet medlemskap i FNO. «Blåboka» legger føringer for hvilke aktører som kan delta i de ulike FOIene og betalingstjenestene. En kan også få særskilt tillatelse til å delta av Bits AS. Dette gjelder FOIene BankID, BankAxept, BALTUS 2.0 og betalingstjenestene eFaktura, AvtaleGiro, AutoGiro og straksbetalinger (Bits AS, 2018d, 2018g, 2018h, 2018i, 2018j, 2019). Betalingsformidlingens selvregulering bidrar dermed til en konsekvensreduksjon da en rekke aktører ikke får kunne delta. Samtidig kan dette bidra til å innvirke på hvorvidt hendelser kan oppstå i form av en hindring, jf. Hollnagel (2004) karakteristikk. Videre opereres det med selvsertifisering og egenevaluering blant bankene deltakende i NICS. Slike aktiviteter favner under Reason (1997, s. 8) betegnelse for myke barrierer, herunder gir dette deltakere selvinnsikt om egen drift og sikkerhet knyttet til deres virke og løsninger (Bits AS, 2018a, s. 21). Videre er det indisier som peker på at foretakene deltar i trening, øvelser og testing av eksisterende beredskapsløsninger (ibid., s. 17-18). Noe som igjen underbygger troen om at myke barrierer bidrar til reduserte konsekvenser ved inntog av nye aktører. En kan til tross for hemmelighold rundt logiske, fysiske og alarmerende barrierer i interbanksystemet se eksempler på bruk av harde barrierer. En indikasjon på bruk av harde logiske barrierer er at meldingsstandardene BOLS og NIBE nå skal krypteres (Bits AS, 2018a, s. 12). En slik forbedring av sikkerhet i meldingsutveksling kan favne innunder betegnelsen harde barrierer (Reason, 1997, s. 8).

Barriereperspektivet kan også benyttes til å belyse bankenes egne særegne løsninger. Bankene oppleves å ha gode tekniske barrierer som hindrer digital kriminalitet (Finanstilsynet, 2018, s. 16). Nedgangen i tekniske brudd på bankenes nettbankløsninger er grunnet bankenes fokus på nettopp logisk sikring av løsning, herunder vil en derfor ikke forvente tekniske angrep mot bankenes løsninger.

Bankene

Interbanksystemet presentert ovenfor illustrerer hvordan barrierer, særlig myke, passive og til dels aktive, vil hemme innvirkningen nye aktører vil ha på norsk betalingsformidling. Synet knyttet til nye aktørers innvirkning, særlig gjennom open banking og PSD2, er også illustrert fra informantene som begrenset. De dempede konsekvensene kan tillegges de strenge reguleringene som, særlig ved PSD2, pålegges nye aktører som ønsker seg inn i markedet for betalingsformidling (Finanstilsynet, 2019, s. 16). Herunder er krav knyttet til sikkerhet, både til bankenes utforming av grensesnitt og sikkerhet i tredjepartenes løsninger sentralt. Indikasjonene som foreligger tilsier at nye aktører som gjennom PSD2-reguleringen ikke vil utfordre eller skape nye sårbarheter og i så måte ikke medføre konsekvenser for samfunnssikkerheten.

Myke barrierer vil begrense inntoget av nye aktører, begrensning av nye aktører kan i all hovedsak skyldes reguleringene og kravene som foreligger til sikkerhet og tilstrekkelige løsninger. Herunder vil en kunne forvente at aktørene som inkluderes i betalingsformidlingen til å ikke være uvørne aktører og dermed ikke innvirke negativt på samfunnssikkerheten. Noe som kan undergrave et slikt poeng knyttes til at aktører som gis sertifikat for PSD2-grensesnittene kan få konsesjonen utenlands og dernest melde grensekryssende virksomhet til Norge (Finanstilsynet, 2019, s. 17). Norske aktører har ikke kontroll over tilsynsmyndigheter i andre land, en kan derfor stille et tankekors til hvorvidt myke barrierer i norsk betalingsformidling forhindrer introduksjon av potensielt uvørne aktører. På en annen side benytter alle tilsynsmyndighetene innen EØS det samme regelverket ved vurdering av konsesjon til tredjepartsaktører PSD2. Et videre moment som kan undergrave sikkerheten fra myke barrierer er open banking og outsourcing. Begge disse aktivitetene belager seg på foretakenes egne strategiske beslutninger, herunder kan det foreligge avgjørelser som ikke nødvendigvis samsvarer med anbefalinger og eksisterende reguleringer. Derfor kan aktører som ikke nødvendigvis omfattes av eksisterende regler og reguleringer introduseres til betalingsformidling og dermed svekke samfunnssikkerheten. Samtidig kan det pekes på at foretakene, særlig de større, besitter vesentlig bestiller-kompetanse og gjennomfører risikoanalyser ved slike avgjørelser. Dette er noe som underbygger foretakenes evne til å fatte rimelige og tilstrekkelige beslutninger som favner deres sikkerhet og risiko. Outsourcing er også i en viss grad omfattet reguleringer, og i så måte barrierer. Aktiviteter knyttet til outsourcing er i stor grad underlagt tilsyn av Finanstilsynet jf. Finanstilsynsloven (1956) § 4 c., samt reguleringer i form av lov og forskrifter som omfatter hvilke deler av verdikjeden

som kan settes ut. Herunder vil en kunne si at outsourcing er omfattet av både aktive og passive myke barrierer (Aven et al., 2004, s. 122; Kjellén, 2000, s. 86; Reason, 1997, s. 8).

Fallgruver ved barrierer

Reason (1997) understreker også at det foreligger en rekke fallgruver knyttet ved barrierer, ergo foreligger det et paradoks knyttet til rasjonale om å sikre ens produktive aktiviteter. Tilbakeholdelse av informasjon knyttet til hendelser er svakhet ved barrierer Reason (1997, s. 55) poengterer, i tilfeller kan barrierene sitte på informasjon av relevans. Herved er det problematisk for operatøren å få tilsyn og informasjon om hendelsen, latente forhold kan som en konsekvens av dette oppstå. Ergo vil sårbarheter i systemet kunne bygge seg opp over lengre tid. Det foreligger ikke tilstrekkelig empirisk belegg som indikerer at dette er beskrivende for barrierene i betalingsformidlingen. Reguleringer pekes også på som en potensiell fallgruve som kan hemme operatører, herunder foretak, sin evne til å operere et system (ibid., s. 49). Problematikken kan særlig oppstå under stressituasjoner som avviker fra normaldrift, som tidligere poengtert er norsk betalingsformidling forskånet fra slike hendelser. Ergo gir dette manglende indisier om hvorvidt reguleringer er hemmende for foretakenes evne til å drifte sine funksjoner. Den omfattende reguleringen som omfatter betalingsformidling gir dog vesentlige retningslinjer for hvordan foretakene skal betjene sine funksjoner. Samtidig kan en vurdere at selvregulering gjennom FNO (NOU 2015:13, s. 169-170) vil være bidragsytende i at reguleringene ikke opptrer hemmende for foretakenes evne til å yte sine funksjoner.

6.1.3 Hvordan blir bankenes arbeid med sikkerhet og beredskap preget av endret aktørbildet?

Prinsippene for samfunnssikkerhets- og beredskapsarbeid er hensiktsmessig for vurdering av hvordan nye aktører i betalingsformidlingen påvirker foretakenes sikkerhetsarbeid. Herunder vil prinsippene påvirkes ulikt grunnet deres veiledende funksjon. Generelt kan en si at aktører introdusert via outsourcing preger foretakenes beredskaps- og sikkerhetsarbeid, mer enn hva nye aktører introdusert gjennom PSD2 eller open banking.

Økende integrering av nye aktører inn i og som tillegg i verdikjeden vil ha innvirkning på arbeidet med sikkerhet, deriblant skape utfordringer. Eksempelvis vil ansvarsprinsippet som peker på at ansvarshaver i normalsituasjon også vil være ansvarsbærende i ekstraordinære situasjoner (Justis- og politidepartmentet, 2002, s. 4) utfordres. Knyttet til betalingsformidling og konsesjonen som er nødvendig for å yte betalingstjenester (Finansforetaksloven, 2015, kapittel 2), vil ansvaret for funksjon på konsesjonsbelagte tjenester falle på bankene. Ansvarsprinsippet tilsier også at ansvaret inkluderer forberedelser knyttet til

beredskapsarbeid, inkludert opprettholdelse under og gjenopprettelse av funksjon etter en hendelse (Engen et al., 2016, s. 282; Justis- og beredskapsdepartementet, 2012, s. 39). Aktørene som yter betalingstjenester, banker inkludert, vil derfor ha ansvaret for å sikre planer, løsninger og generelle forberedelser for å være godt rustet i stressituasjoner. Prinsippet om ansvar er også tydeliggjort i ansvaret bankene har i grensesnittet som gis ut i sammenheng med PSD2, bankene må søre for at sikkerheten i løsningen er tilstrekkelig (Finanstilsynet, 2019, s. 49).

Outsourcing og open banking kan innvirke på ansvarsprinsippet ved at flere ansvarsbærere i verdikjeden kan komplisere forholdene. Foretakenes manglende kompetanse knyttet til bestilling og avtaleinngåelse gjør ansvarsavklaring mer pressende (Finanstilsynet, 2019, s. 31). Særlig ved outsourcing kan ansvarsprinsippet utfordret, ettersom underleverandører overtar leveranse av tjenesten (Power et al., 2006, s. 3). En avklaring ved avtaleinngåelse blir derfor nødvendig for å avklare ansvarsforholdet aktørene imellom. Problemet med ansvarsprinsippet og ansvarshaver blir ytterligere prekært ved offshoring. Tjenesten driftes da av en underleverandør som ikke er underlagt norsk regulering og reglement. Foretaket sitter ergo med ansvaret for tjenestens funksjonalitet, men ikke nødvendigvis med ansvaret for at aktiviteter underlagt funksjonen opprettholdes i stressituasjoner. En vil da oppleve problemer med å være ansvarlig for arbeidet med opprettholdelse, gjenopprettelse og beredskapsarbeid tilknyttet funksjonen (Norges Bank, 2018a, s. 7).

Likhetsprinsippet som underbygger ansvarsprinsippet kan ved outsourcing virke mot sin opprinnelige hensikt. Om prinsippet følges slavisk vil det innebære at foretakene må belage seg på underleverandørers evne til å håndtere hendelse, da organisasjonen skal i krisesituasjon operere så likt som mulig organisasjon i daglig drift (Justis- og beredskapsdepartementet, 2012, s. 39; Justis- og politidepartmentet, 2002, s. 4). Dette innebærer at foretakene i norsk betalingsformidling i vesentlig grad vil være avhengig av tjenester fra utlandet. Problematikken ved håndtering av hendelser blir videre tydelig ved nye aktører introdusert gjennom PSD2 og open banking i henhold til nærhetsprinsippet. Her vil det da være nye aktører med ansvaret for forberedelse og håndtering av hendelser.

Nærhetsprinsippet tilsier at hendelser skal håndteres på som lavt nivå som mulig (Justis- og beredskapsdepartementet, 2012, s. 39; Justis- og politidepartmentet, 2002, s. 4). Her vil hendelsen i henhold til prinsippet håndteres av aktører som inngår i verdikjeden for betalingsformidling, men samtidig ikke har overordnet ansvar for tjenestens funksjon og virke. Derfor vil igjen foretaket måtte belage seg på underleverandører eller andre aktører som

inngår i verdikjeden for betalingsformidling. Dog bør det poengteres at ved PSD2 foreligger ansvaret for håndtering av hendelser i større grad hos aktørene som har konsesjon til å knytte seg opp mot grensesnittet. Outsourcing er dog en noe som utfordrer denne problematikken, samtidig kan et ytterligere problem tillegges dersom foretaket har kompetansebortfall, noe som preger enkelte foretak (Finanstilsynet, 2019, s. 39). Kompetansebortfall kan bidra til at bankene ikke nødvendigvis besitter tilstrekkelige kunnskap eller ressurser til å håndtere eller planlegge for en hendelse (Finanstilsynet, 2019, s. 55). Logikken om nærhet som prinsippet bygger på (Engen et al., 2016, s. 283), vil da bortfalle og de som best håndterer hendelsen er utenfor foretaket. Det oppstår her et gap mellom prinsippet om ansvar, nærhetsprinsippet og ansvaret til konsesjonsbelagte tjenester da disse ikke nødvendigvis ikke tar høyde for bortfall av kunnskap i foretaket som har konsesjon for tjenesten. En løsning på problematikken kan være kunnskapsoverføring mellom foretak og underleverandør, selv om dette kan være en krevende prosess (Gottschalk, 2013, s. 26).

Prinsippet om samvirke blir også utfordret av nye aktører i verdikjeden for betalingsformidling, særlig dersom foretaket har en uoversiktlig verdikjede. I tilfeller hvor foretaket operer med en kompleks verdikjede som inkluderer flere underleverandører og vanskelig å se i en lineær rekke (Gottschalk, 2013, s. 17), vil samordning bli komplekst. En kan derfor vurdere hvordan banker kan etterleve samvirkeprinsippet, som etterspør at ansvarshavende aktør sikrer samvirke med relevante aktører (Justis- og beredskapsdepartementet, 2012, s. 39). Uttømmende outsourcing kan skape problemer for foretakene i å styre, sikre kommunikasjon og rolleavklaring for beredskap og i krisesituasjoner (Finanstilsynet, 2018, s. 8). Prinsippet tydeliggjør videre behovet aktører har i å kartlegge avhengigheter av deler på alle nivå og hvilke aktører som er nødvendige for forebyggende arbeid (Justis- og beredskapsdepartementet, 2012, s. 39). Verdikjedens økende kompleksitet kan gjøre denne prosessen vanskeligere og i så måte hemme foretakenes arbeid knyttet til sikkerhet og beredskap. Problemet med å sikre samvirke oppleves som mer problematisk i tilfeller ved offshoring, her vil faktorer som språk, kulturelle forskjeller og geografisk avstand også innvirke på avtaleforholdet (Gottschalk, 2013, s. 26). Ergo, kan det være vanskelig for foretaket å opprettholde eller gjenopprette funksjoner ved eller etter en stressituasjon (Finanstilsynet, 2019, s. 55).

Myndighetene har ved flere tilfeller oppfattet at foretakene i betalingsformidling ikke har tilstrekkelig beredskapsløsninger i sine løsninger (Finanstilsynet, 2019, s. 22). Om dette skyldes bankenes manglende oversikt over egne verdikjeder, manglende kompetanse eller

mangelfulle avtaler med underleverandører er vanskelig å si noe om. En kan derimot vurdere at nye aktører inkludert inn i verdikjeden, gjennom PSD2 og open banking til i en viss grad innvirke på beredskaps- og samfunnssikkerhetsarbeidet. Outsourcing har vært en aktivitet foretakene har bedrevet i lengre tid, og har derfor større innvirkning i dag og mest sannsynlig. En kan derimot vurdere foretakenes kompetanse til å bestille og følge opp tjenester de har outsourcet som en aktivitet som i større grad vil behjelpe de i å etterleve prinsippene om samfunnssikkerhet- og beredskapsarbeid. Utfordringene knyttet til arbeid med sikkerhet og beredskap er ventet å være størst knyttet til ansvars- og samvirkeprinsippet. Problematikken knyttet til foretakenes manglende bestiller-kompetanse (ibid., s. 31) vil innvirke på flere faktorer enn tjenesteleveranse utover sikkerhet- og beredskapsarbeid.

6.2 Hvordan innvirker nye aktører i betalingsformidlingen samfunnssikkerheten?

Det er nå drøftet omkring hvordan nye aktører innvirker på den eksisterende sikkerheten i norsk betalingsformidling. Herunder er det avdekket at til tross for at nye utfordringer presenteres for foretakene utgjør ikke nye aktører i norsk betalingsformidling et uhåndterbart sikkerhetsproblem. Uansett utgjør nye aktører utfordringer som kan ha innvirkning på samfunnssikkerheten, dette kapittelet ser på hvordan og i hvilket omfang. Studiens mål var å besvare problemstillingen presentert innledningsvis i kapittel 1.2, studiens problemstilling utledes således.

Hvilke potensielle konsekvenser kan introduksjon av nye aktører i betalingsformidlingen ha for samfunnssikkerheten?

Derfor blir analysen fra 6.1 løftet til å gjelde samfunnssikkerheten hvor betalingsformidling er omfattet (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 85). Det er da nærliggende å benytte sentrale begrep og definisjoner innen samfunnssikkerheten.

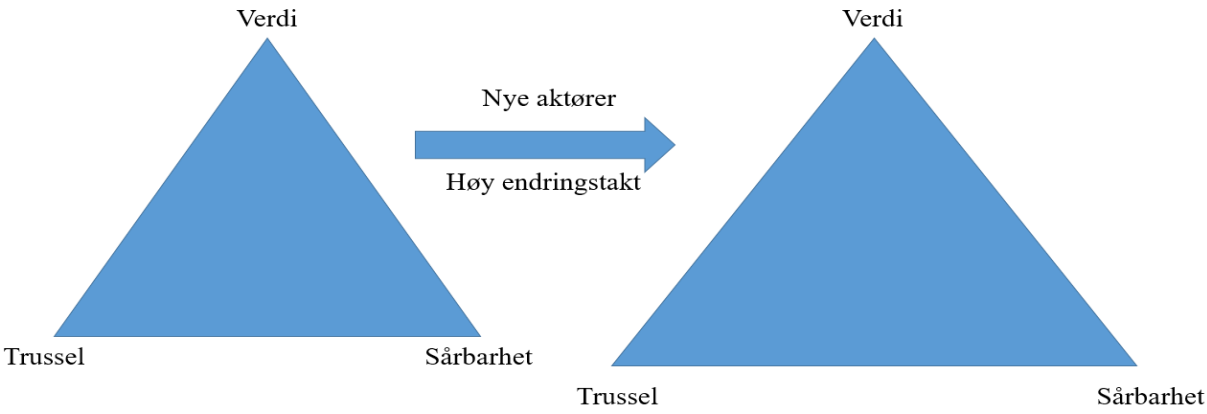
Risiko for samfunnet, grunnet nye aktører

Risiko i henhold til definisjonen presentert av Aven og Renn (2010, s. 3) presenterer faktorer som kan benyttes for å belyse risikoen knyttet til at nye aktører tar del i norsk betalingsformidling. Sentral i definisjonen er usikkerhet. Vurderinger omkring innvirkningen nye aktører vil ha på sikkerheten kan sies å være preget av usikkerhet. Det kan ikke underdrives at vurderingene gjort i studien har usikkerhet tilknyttet seg. Usikkerheten kan beskrives som epistemisk, da det tilstrekkelig grad ikke foreligger tilstrekkelig empiriske indikasjoner om gjennom hvilke mekanisme nye aktører utfordrer samfunnssikkerheten. Ei heller i hvilken grad. Betegnelsen epistemisk usikkerhet blir derfor passende da vurderinger

omkring risikoagenten vil preges av kunnskapsmangel (ibid., s. 78). Herunder kan risikoen knyttet til nye aktører også tillegges egenskapen kompleksitet, som da viser til vanskeligheter ved å avdekke kausalkjeder som igjen vanskeliggjør analyse (Renn, 2008, s. 186).

Til tross for dette har FS1, FS2 og den påfølgende analysen knyttet til FS3 indikert at det foreligger en risiko knyttet til introduksjon av nye aktører. Endringstakten i seg selv ansees som en risikobærer ettersom dette involverer endringer i aktørbilde, reguleringer og teknologiske løsninger (Finanstilsynet, 2018, s. 11). En kan samtidig grunnet alle barrierene som omringer betalingsformidlingen at konsekvensene tilknyttet risikoen er ikke er stor. Konsekvenser som viser til størrelse, utbredelse intensitet og omfang ved en hendelse (Engen et al., 2016, s. 81), herunder favner problemstillingen og besvarelsens fokus. Manglende alvorlighet tilknyttet konsekvensene ved hendelser, forbundet med nye aktører i betalingsformidlingen er grunnen til at risikoen vurderes som lav. Men som poengtert er vurderingen tilknyttet epistemisk usikkerhet grunnet risikoagentens kompleksitet og generell usikkerhet i kunnskaps- og informasjonsgrunnlaget.

I en alternativ risikovurdering kan en se at risikoen knyttet til nye aktører blir annerledes. Trefaktormodellen tar til betraktning tre faktorer i sin beskrivelse av risiko. Faktorene vektlegges ulikt avhengig av system (Nasjonal Sikkerhetsmyndighet, 2015, s. 12).



Figur 14, endringer i risiko. Trefaktormodellen av NSM, Sikkerhetsfaglig råd, 2015 som gjengitt i NOU 2016:19 (s. 44)

Verdi, i henhold til Engen et al. (2016, s. 81) forståelse viser til noe mennesket verdsetter, dette kan variere i henhold til systemet en ser på. Herunder bli betalingssystemets økende integrasjon i samfunnet noe som øker verdidimensjonen. Ergo vil risikoen øke sammen med avhengigheten av tjenesten. Sårbarhet jf. Engen et al. (2016, s. 47) og Renn (2008, s. 69) viser til hvordan et system vil fungere ved og etter en hendelse. Potensielle sårbarheter ved inntoget av nye aktører er avdekket og kan potensielt øke og skape nye sårbarheter, som

konsentrasjonsrisiko i nye løsninger, bortfall av kompetanse og manglende sikkerhet i open banking-grensesnitt. Potensiell fremtidige sårbarheter kan derfor øke ved nye aktører. Samtidig er FOIer og betalingstjenestene omkranset av myke barrierer, noe som reduserer sårbarheten, gjennom tilgjengeligheten til sentrale funksjoner. Trusselbildet er som en følge av nye aktører, er også ventet å utvides. Tredjepartsleverandører kan benyttes som en kanal for hackerangrep rettet mot bankene (EBA, 2018, s. 8). Samtidig vil den internasjonale økningen i cyberangrep mot bankene (Finanstilsynet, 2018, s. 21) indikere at risikoen knyttet til betalingsformidling er tiltakende. Bruk av trefaktormodellen gir et annerledes syn på hvorvidt risikoen i betalingsformidling da denne i større grad vurderer faktorer som innvirker på risikoen. Differensieringen gjør en derfor i stand til å til å se hvordan risikoen for hendelser endres noe fra en definisjon til enn annen.

Risikoforståelsene indikerer ulik gradering av risiko ved introduksjon av nye aktører til norsk betalingsformidling. Bruk av perspektivene presenterer en mer holistisk vurdering av risikoen. Herunder om den er tiltakende, usikkerhet tilknyttet vurderingen, hvordan risikoen innvirker på ulike faktorer av betydning for fremtidig risikobilde og legger så grunnlag for en mer hensiktsmessig vurdering. Betalingsformidlingen i lys av Aven og Renn (2010, s. 3) tolkning og trefaktormodellen (Nasjonal Sikkerhetsmyndighet, 2015, s. 12; NOU 2016:19, s. 44) kan forventes å oppleve en endring i risikobildet. Introduksjonen av nye aktører, les: økt angerepsflate, vil sammen med det internasjonale trusselbilde med flere cyberangrep øke risikoen (EBA, 2018, s. 8; Finanstilsynet, 2018, s. 12). Barrierene som omringer sentrale funksjoner og FOIer i norsk betalingsformidling er samtidig sentralt i vurderingen. Gjennom streng reguleringer omkring involvering og inkludering av nye aktører knyttet til verdikjeden kan det forventes at sårbarheter nye aktører mulig bringer med seg ikke videreføres til sentrale funksjoner. Ergo vil en kunne vurdere at bortfall av FOIene og andre sentrale funksjoner, som ville innvirket på samfunnssikkerheten (Finanstilsynet, 2018, s. 28), som en konsekvens av nye aktører som lite trolig.

Følgelig vil systemrisikoen, i henhold til forståelsen presentert av Renn (2008, s. 5), ha en lignende vurdering av risikoen. Systemrisikoen i betalingsformidlingen vil ikke i nær fremtid bli påvirket av nye aktører. Det er grunnet strenge krav ved PSD2 som både stiller krav til tredjepartsaktører og begrenser tilgangen de får gjennom et standardisert grensesnitt.

De vil ikke få tilgang til det samme som bankene, men de vil få tilgang til et standardisert grensesnitt på toppen av bankene, som de kan bruke til betalinger. (Informant 21).

Nye aktører og potensiell risiko knyttet til deres virksomhet vil således ikke nødvendigvis ha kaskadeeffekter på andre funksjoner i betalingssystemet, enn sin egen. At konsekvensene ikke forventes å smitte over til andre aktører begrenser systemrisikoen (IRGC, 2018, s. 9). Tredjepartenes begrensede tilgang via grensesnittet som bankene tilbyr gjennom PSD2 presenterer derfor ikke en videre systemrisiko, med mindre enn konsentrasjon av brukere blir ytterst avhengig av tredjepartsleverandørens tjenester. Open banking og outsourcing kan medføre en tettere integrering av nye aktører gjennom bi- og multilaterale samarbeid som i tilfeller inngår i bankenes verdikjede (Evry AS, 2017, s. 24; Gottschalk, 2013, s. 17). Kaskadeeffekter som følge av manifestering av risiko vil sammenheng være mer plausibelt, særlig ved outsourcing som innvirker på foretakenes leveranse av tjenester.

Systemrisiko i norsk betalingsformidling er tilstedeværende, grunnet konsentrasjonsrisiko rundt noen få leverandører knyttet til sentrale tjenester og FOIer (NOU 2015:13, s. 170). At flere av leverandørene er samlokalisert med hverandre underbygger systemrisikoen (Norges Bank, 2018a, s. 7, 28), særlig ved fysisk angrep. Hendelser vil her kunne innvirke på betalingsformidlingen i stor grad, noe som ville medført vesentlige konsekvenser nasjonalt (Finanstilsynet, 2018, s. 29). Hvorvidt systemrisikoen er bekymringsverdig for betalingsformidlingen er grunnet dets kompleksitet vanskelig å konkludere. Risikoen er tilknyttet usikkerhet og kompleksitet, noe som systemrisikoer gjerne er (Renn et al., 2011, s. 234). Samtidig kan betalingsformidlingen samlet sett, grunnet lovpålegget om kontantberedskap (Finansforetaksforskriften, 2017, § 16-7), redusere systemrisikoen vesentlig da betalingsmidler i samfunnet fortsatt foreligger ved bortfall av elektroniske løsninger (Finanstilsynet & Norges Bank, 2016, s. 4). En kan dermed, ved bortfall av elektronisk betalingsformidling, ha løsninger som vil redusere risikoen befolkningen ellers vil oppleve i henhold til å anskaffe elementære varer. Hvorvidt bankenes etterlevelse av lovpålegget er i tilstrekkelig grad foreligger det ingen empiriske indikasjoner på, ergo vanskelig å vurdere.

Innvirkning på samfunnssikkerheten

Avslutningsvis kan en av diskusjonen ovenfor vurdere hvordan samfunnssikkerheten preges av endringer i aktørbildet for betalingsformidling. Definisjonen som ligger til grunn er:

> *Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare (Justis- og beredskapsdepartementet, 2016, s. 9).*

Samfunnets evne i denne sammenheng viser til aktørene, herunder Norges Bank, Finanstilsynet, FNO, Bits AS, banker og betalingsforetak og deres underleverandører jf. figur

7, i norsk betalingsformidling og deres evne til å verne om funksjonene i betalingsformidling. En kan på bakgrunn av diskusjoner og overveielser i kapittelet vurdere at disse aktørenes evne til å verne om funksjonen betalingsformidling som god. Bakgrunnen for dette kan tillegges de omfattende reguleringene som legger føringer for konsesjonsgrunnlag, adgang til systemer og atferd blant aktørene (Finansforetaksloven, 2015; Finanstilsynsloven, 1956). En kan samtidig vurdere foretakenes evne, herunder beredskap, til tross mangler (Finansdepartementet, 2018a, s. 89; Finanstilsynet, 2019, s. 22), til å være tilstrekkelig. Lovpålegget i Finansforetaksforskriften (2017, § 16-7) underbygger evnen aktørene har til å opprettholde funksjonen ved hendelser som truer. Mange av foretakenes deltakelse i NFCERT gjør også betalingsformidlingen bedre rustet, ergo evne, i å håndtere hendelser og generell oversikt i trusselbildet (Finans Norge, 2019).

Først og fremst vil ikke PSD2 og aktørene som introduseres i betalingsformidlingen medføre seriøs risiko og konsekvenser. Dette til tross for at angerepsflaten jf. trefaktormodellen kan forventes å bli større. Årsaken til at PSD2 ikke innvirker vesentlig på samfunnssikkerheten kan tillegges tilgangen nye aktører får gjennom grensesnittet, nye aktører trenger konsesjon og sertifikat for å få tilgang til sertifikatet. Forventningen om moderat fremvekst av aktører tilknyttet PSD2 (Finanstilsynet, 2019, s. 16) underbygger deres ventede innvirkning på samfunnssikkerheten.

Open banking stiller litt større krav til bankene aktørenes introduseres til betalingsformidling via en eller flere banker (Evry AS, 2017, s. 24). Grensesnittet slike aktører kan få tilgang til behøver ikke, til tross for anbefalinger, å følge retningslinjene fastsatt i PSD2. Bankene og utviklere av grensesnittet blir her ansvarlig for å påse at løsningen har tilstrekkelig sikkerhet. Samtidig må banken vurdere hva og til hvilken grad nye tredjepartsleverandører skal få tilgang til gjennom grensesnittet. Her vil innvirkningen på samfunnssikkerhet ligge i bankenes evne til å vurdere hva som er sentralt for ens funksjon.

Outsourcing presenterer de mest pressende problemene for norsk betalingsformidling og samfunnssikkerheten. Foretakenes eksiterende outsourcing av tjenester er til dels konsentrert rundt et fåtalls av leverandører, noe som skaper en konsentrasjonsrisiko (NOU 2015:13, s. 170). Videre vil outsourcing direkte innvirke på verdikjeden levert av foretak som yter betalingstjenester, noe som kan gjøre foretakene avhengig av eksterne aktører. Samtidig kan en forvente at kompleksiteten i verdikjeden øker ved outsourcing (Gottschalk, 2013, s. 17), noe som svekker foretakenes styringsevne. I tillegg kan en risikere at viktig kompetanse knyttet til drift og utvikling av tjenester og funksjoner kan bortfalle, en slik trend

problematiserer foretakenes evne til å opprettholde tilstrekkelig nivå på tjenesten og eller funksjonen (Finanstilsynet, 2019, s. 39). Herunder svekkes «samfunnets evne» til å kunne håndtere hendelser, noe som svekker samfunnssikkerheten.

Generelt kan en derimot si at foretakenes evne til håndtering og opprettholdelse av funksjoner oppleves til å være tilstrekkelig. Kombinert med den begrensede tilgangen nye aktører forventes å få, kan en derfor ikke konkludere med at samfunnssikkerheten vil preges nevneverdig som en følge av inntoget av nye aktører i betalingsformidlingen.

6.3 Framtidsutsikter for norsk betalingsformidling

I nærmeste fremtid foreligger det indikasjoner på at en ikke kan forvente at nye aktører vil medføre signifikante konsekvenser for sikkerheten i betalingsformidlingen. PSD2-direktivet som åpner for en rekke nye aktører vil ha en moderat effekt med tanke på antall nye aktører inn i betalingsformidlingen (Finanstilsynet, 2019, s. 16). Et videre moment er at aktører som gjennom enten PSD2, eller bi- eller multilaterale open banking samarbeid vil tilby tjenester «utenpå» bankenes løsninger. Herved vil den nye forretningsplattformen ikke fragmentere eksisterende verdikjeder. Videre burde det poengteres at det forventes at bankene selv forventes å være de mest fremtredende aktørene knyttet til bruk av PSD2-grensesnittet. Allerede er det introdusert løsninger fra banker som gir tilgang til konto i andre banker (Norges Bank, 2019, s. 10). Heller vil man ikke oppleve at nye tjenestetilbydere vil ha tilgang til interbanksystemet med mindre de har konsesjon til å operere som et betalingsforetak, finansinstitusjon eller særskilt tillatelse (Betalingssystemloven, 1999, kapittel 5; Bits AS, 2018c, s. 2).

Internasjonale trender som indikerer en økning i cyberangrep (Finanstilsynet, 2018, s. 21), kan sammen med nye tredjepartsaktører og –leverandører på sikt medføre en trussel. En kan derimot kunne forvente at målrettede angrep mot tredjepartstilbydere som forsøk på å tilgang til bankenes infrastruktur og systemer. En kan også tenke seg at kriminelle handlinger knyttet til svindel i større grad kan returnere til det norske markedet, gjennom nye tredjepartstilbydere.

Bigtechaktører kan på sikt utvikle tjenester og et tjenesteutvalg som kan konkurrere på lik linje med bankene. Et tenkt scenario er knyttet til at flere av disse kan opprette e-pengeforetak og egne digitale valutaer som de benytter til transaksjoner på ens plattform (Norges Bank, 2019, s. 11). På sikt kan dette vise seg problematisk, da en potensielt kan få konsentrasjon av norske brukere rundt disse tjenestene, særlig for netthandel, P2P-betalinger og P2B-

betalinger. En kan derimot ikke si om dette vil ha noe særlig innvirkning på dagligvarehandelen og kortbruken i Norge. Et sentralt moment er at det norske finansielle systemet er såpass effektivt, sikkert og raskt at alternative tjenester pr. i dag vil ha vanskeligheter med å utkonkurrere bankenes eksisterende løsninger innenlands.

Nye aktører som introduseres til norsk betalingsformidling gjennom samarbeid eller PSD2 forventes ikke å påvirke samfunnssikkerheten vesentlig, utenom økt eksponering og tendenser til økt omfang av svindel. Framtidsutsiktene blir i større grad påvirket av outsourcing og offshoring. Slike strategiske valg har direkte innvirkning på bankenes verdikjeder for leveranse av tjenester knyttet til betaling. Her kan det forekomme, designes, oppstå og opparbeides en rekke forhold som *kan* ha innvirkning på samfunnssikkerheten. Herunder vil valg som fattes av foretakene kunne få følger for deres evne til å levere tjenester de har konsesjon for. I tilfeller med bortfall av underleverandører kan foretakene finne seg inkapabel til å levere tjenestene, dette vil i siste instans innvirke på brukerne – den norske befolkning. I fremtiden kan en forvente at om trenden knyttet til outsourcing, særlig skytjenester, holder ved lag, at kompleksiteten øker (Finanstilsynet, 2019, s. 55). Ergo kan foretakenes evne, særlig de mindre, oppleve problemer med å implementere hensiktsmessig styring av verdikjeden. Igjen vil en da kunne ha deler eller komponenter i verdikjeden som ikke i tilstrekkelig grad er avdekket og vurdert i henhold til kritikalitet. Problemet blir mer innlysende i tilfeller ved offshoring, hvor tjenestene og leveransen flyttes utenlands. Herunder kan det være flere forhold som problematiserer evnen foretak og relevante myndigheter har til styring, innsyn og kunnskap omkring verdikjeden. Outsourcing *kan* derfor presentere, i nærmeste fremtid, de mest pressende utfordringene knyttet til sikkerhet.

7. Konklusjon og veien videre

Studien har forsøkt å avdekke hvorvidt nye aktørers inntog i norsk betalingsformidling har innvirkning på samfunnssikkerheten i Norge. Problemstillingen som forelå som grunnlag for studien var:

Hvilke potensielle konsekvenser kan introduksjon av nye aktører i betalingsformidlingen ha for samfunnssikkerheten?

I forsøket på å avdekke dette er det identifisert tre hovedsakelige kanaler nye aktører kan inkluderes i norsk betalingsformidling: EU-direktivet PSD2; forretningsplattformen open banking; og aktiviteten outsourcing.

Perrow (1999) sitt rammeverk og tanker om iboende egenskaper ved systemer som kan forårsake *Normal Accidents* gjorde det mulig å analysere norsk betalingsformidling. Fra dette kunne det vurderes at norsk betalingsformidling er et system med en rekke tett koplinger grunnet systemets tidssensitivitet og at komponentene vanskelig kan byttes ut, særlig i interbanksystemet. Videre ble det vurdert at kompleksiteten i systemets interaksjoner ville forventes å øke noe som en følge av nye aktører. Dette kan potensielt øke potensialet for *Normal Accidents.* En kunne derimot ikke argumentere for at egenskapene i systemet for betalingsformidling var iboende da systemets egenskaper gjennom en årrekke er tillagt systemet, noe som er ventet å fortsette. Det foreligger derfor ikke grunnlag til å si at systemulykker er et generelt kjennetegn ved betalingsformidling.

Organisatoriske ulykker, som presentert av Reason (1997) presenterte en alternativ vei å vurdere hvordan systemet som en helhet ville påvirkes av nye aktører. Her ville vurderingen knyttet til systemets potensial for ulykker vurderes i lys av aktive feil og latente forhold. Vanskeligheter i å avdekke aktive feil, førte fokus over på latente betingelser. En kan ved flere tilfeller se hvor latente betingelser kan bygges opp i betalingsformidlingen, gjerne i form av bortfall av kompetanse, styringsevne og økt kompleksitet i verdikjeden. Outsourcing, knyttet til nye og eksisterende leverandører, ble trukket frem som potensielt mest innvirkende. Her vil latente forhold og aktive feil kan ha direkte innvirkning på aktørenes evne til å levere betalingstjenester. Nye tredjepartsaktører forventes å kun ramme dem selv og grunnet forventet utforming av grensesnitt ikke vil medføre kaskadeeffekter med konsekvenser for eksisterende aktører.

Videre ble barrierene i norsk betalingsformidling analysert. Barrierene som foreligger i norsk betalingsformidling vurderes som hensiktsmessig for å begrense konsekvensene nye aktører har på sikkerheten og herunder potensielle negative konsekvenser. Herunder foreligger det en rekke aktiviteter, regler, reguleringer og tilsynsmyndigheter som begrenser de potensielle konsekvensene nye aktører kan ha på betalingsformidlingen. Det har ikke vært mulig å tilstrekkelig vurdere logiske harde barrierer knyttet til betalingsformidling og det kan derfor ikke trekke konkluderende bemerkninger til dette. Videre ble innvirkninger på foretakenes arbeid knyttet til beredskap og sikkerhet som en følge av et bredere aktørbilde vurdert i lys av prinsippene for beredskap- og samfunnssikkerhetsarbeid. Konsekvensene knyttet til nye aktører presenterer enkelte utfordringer for eksisterende aktører i deres beredskap- og samfunnssikkerhetsarbeid, ansvars- og samvirkeprinsippet spesielt. Her ble det avdekket at outsourcing stilte de mest prekære problemene for arbeidet.

Avslutningsvis ble begrepene knyttet til risiko, trefaktormodellen og samfunnssikkerhet benyttet for å belyse innvirkningen nye aktører i betalingsformidlingen har på samfunnssikkerheten. En kunne forvente, stor usikkerhet til tross, at risikoen ved nye aktører ville øke. Vurderingen fattes i stor grad med grunnlag i hvordan risikoen i lys av trefaktormodellen øker som en følge av eksponering og trusselbilde. Samfunnssikkerheten vurderes dog som ikke veldig preget da, samfunnets evne til å håndtere og forberede seg mot hendelser ikke vesentlig hemmes av nye aktører i betalingsformidlingen.

En kan derfor si at samfunnssikkerheten *kan* påvirkes av et sprikende aktørbilde hvor tilbydere av betalingstjenester, banker, fintechs, bigtechs, datasentraler, IT-leverandører og alle disse aktørenes tilhørende underleverandører i symbiose utgjør et ytterst kompleks økosystem. Samtidig grunnet betalingsformidlingens omfattende bruk av myke barrierer vil redusere de potensielle konsekvensene nye aktører kan medføre, særlig i et kortere tidsperspektiv. Noen av konsekvensene ved nye aktører kan ventes å være økt kompleksitet og økt angerepsflate. Konsekvensene er derimot størst knyttet til nye aktørers innvirkning på eksisterende aktørers beredskap- og sikkerhetsarbeid. Outsourcing presenterer her de mest pressende potensielle konsekvensene for samfunnssikkerheten i dag og ventes å gjøre det i nærmeste fremtid. Dette er noe som kan hemme evnen aktørene har til å verne og håndtere hendelser som kan medføre konsekvenser for betalingsformidlingen. I ett lengre perspektiv kan derimot bigtechs presentere utfordringer med konsekvenser for samfunnssikkerheten. Det kan foreligge potensielle konsekvenser til nye aktører om de får en vesentlig konsentrasjon av brukere. En slik utvikling vil medføre konsekvenser for samfunnssikkerheten.

Veien videre, nye potensielle studier

Studien har favnet en rekke tema som introduserer en rekke studier som videre kan vurdere risiko og sårbarheter i norsk betalingsformidling. En potensiell vei videre for å vurdere den totale risikoen for systemsvikt i norsk betalingsformidlingen kan tilknyttes de ulike avtaleforholdene mellom kortutstedere og innløsere av transaksjoner. Her kan det foreligge bilaterale avtaler og forhold som kan ytterligere komplisere et allerede komplekst bilde. Videre er det kjent at datasentralene som betalingsforetak og banker benytter seg av i Norge er få og store, dette skaper en konsentrasjonsrisiko. Dersom en av disse datasentralene skal falle bort over en lengre tidsperiode grunnet noe uforutsett ville dette fått store ramifikasjoner for store deler av betalingsinfrastrukturen i Norge. Det kunne derfor videre være hensiktsmessig å utlede en studie knyttet til hvordan norsk betalingsformidling alternativt kunne redusert denne sårbarheten. Alternativt kan en studie se konkret på avtaleforholdet mellom finansforetak og underleverandører. Her kan avtalemessige vurderinger og forholdet i praksis vurderes for å få innlysende innsikt i om og eventuelt hvilken grad outsourcing kan produsere sårbarheter og risiko i norske foretaks verdikjeder for betalingstjenester. Sistnevnte kan dog gå noe innover Finanstilsynets mandat.

Avslutningsvis vil jeg poengtere at etter mitt syn og nå kunnskap, mener jeg at betalingsformidling favner innunder og derved burde inkluderes i hva Direktoratet for samfunnssikkerhet og beredskap (2016, s. 8) betegner som funksjoner kritisk for samfunnets funksjonalitet. Avvik og eller hendelser knyttet til betalingsformidling som medfører bortfall over syv eller færre døgn vil ha ringvirkninger av betydning for samfunnets funksjon. Ergo kan betalingsformidling vurderes som en kritisk samfunnsfunksjon.

Referanseliste

Andersen, Espen & Sannes, Ragnvald. (2018). Er du klar for digitalisering? *Praktisk økonomi & finans*, *34*(3), 196-213. doi:10.18261/issn.1504-2871-2018-03-04

Aven, Terje. (2006). *Pålitelighets- og risikoanalyse* (4. utg. utg.). Oslo: Universitetsforl.

Aven, Terje, Boyesen, Marit, Njå, Ove, Olsen, Kjell Harald & Sandve, Kjell. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.

Aven, Terje & Renn, Ortwin. (2010). *Risk management and governance : concepts, guidelines and applications* (Vol. volume 16). Heidelberg: Springer.

Bakken, Jonas Blich. (2018, 23.01.18). Taper på første tjeneste – skal tjene på å kutte regninger. Hentet fra https://www.dn.no/handel/payr/espen-einn/kyrre-overland-andersen/taper-pa-forste-tjeneste-skal-tjene-pa-a-kutte-regninger/2-1-256748

BankID. (ingen dato(a)). BankID-Partnere. fra https://www.bankid.no/bedrift/kom-i-gang/bankid-partnere/

BankiD. (ingen dato(b)). xID. fra https://www.bankid.no/privat/los-mitt-bankid-problem/xid/

Betalingssystemloven. (1999). *Lov om betalingssystemer m.v. (LOV-1999-12-17-95).* Hentet fra https://lovdata.no/dokument/NL/lov/1999-12-17-95.

Bits AS. (2016a). *Nyhetsbrev April 2016 - ISO 20022 prosjektet*. Hentet fra https://www.bits.no/wp-content/uploads/2016/07/Nyhetsbrev_1-Bits-ISO-20022-prosjektet.pdf.

Bits AS. (2016b). *Nyhetsbrev Sommeren 2016 - ISO 20022*. Hentet fra https://www.bits.no/wp-content/uploads/2016/07/Nyhetsbrev_2-Bits-ISO-20022-prosjektet.pdf.

Bits AS. (2018a). *Årsrapport for NICS 2018*. Hentet fra https://www.bits.no/document/arsrapport-for-nics-u-vedlegg/

Bits AS. (2018b). *Regler for avregning og oppgjør av transaksjoner som inngår i Norwegian Interbank Clearing System (NICS)*. Hentet fra https://www.bits.no/document/regler-om-avregning-og-oppgjor-for-transaksjoner-som-inngar-i-nics/.

Bits AS. (2018c). *Alminnelig regelverk om interbanktransaksjoner ved innenlands betalingsformidling*. Hentet fra https://www.bits.no/document/alminnelig-regelverk-om-interbanktransaksjoner-ved-innenlandsk-betalingsformidling/.

Bits AS. (2018d). *Regler om BALTUS*. Hentet fra https://www.bits.no/document/regler-om-baltus/.

Bits AS. (2018e). *Driftsmønster for NICS*. Hentet fra https://www.bits.no/document/driftsmonster-for-nics-vedlegg-1-til-regler-om-avregning-og-oppgjor-av-transaksjoner-som-inngar-i-nics/.

Bits AS. (2018f). *Tiltak ved omfattende avvik i betalingsinfrastrukturen* Hentet fra https://www.bits.no/document/tiltak-ved-omfattende-avvik-i-betalingsinfrastrukturen-vedlegg-6-til-regler-om-avregning-og-oppgjor-av-transaksjoner-som-inngar-i-nics/.

Bits AS. (2018g). *Regler om BankID*. Hentet fra https://www.bits.no/wp-content/uploads/2018/04/Regler-om-BankID-15.03.2018-1.pdf.

Bits AS. (2018h). *Regler for AutoGiro*. Hentet fra https://www.bits.no/document/regler-for-autogiro/.

Bits AS. (2018i). *Regler om AvtaleGiro*. Hentet fra https://www.bits.no/document/regler-om-avtalegiro/.

Bits AS. (2018j). *Regler om BankAxept infrastruktur*. Hentet fra https://www.bits.no/document/regler-om-bankaxept-infrastruktur/.

Bits AS. (2018k). *Tidsfrister for avvikshåndtering ved manglende dekning*. Hentet fra https://www.bits.no/document/tidsfrister-for-avvikshandtering-ved-manglende-dekning-vedlegg-2-til-regler-om-avregning-og-oppgjor-av-transaksjoner-som-inngar-i-nics/.

Bits AS. (2018l). *Regler om innenlandske kreditoverføringer mellom banker*. Hentet fra https://www.bits.no/document/regler-om-innenlandske-kreditoverforinger-mellom-banker/.

Bits AS. (2018m). Blåboka gjenoppstår i Bits-drakt! Hentet 29.05, 2019, fra https://www.bits.no/blaboka-gjenoppstar-i-bits-drakt/

Bits AS. (2019). *Regler om eFaktura*. Hentet fra https://www.bits.no/document/regler-for-efaktura-tjenesten/.

Bits AS. (ingen dato(a)). Autogiro. Hentet 14.03., 2019, fra https://www.bits.no/bank/autogiro/

Bits AS. (ingen dato(b)). AvtaleGiro. Hentet 29.03, 2019, fra https://www.bits.no/bank/avtalegiro/

Bits AS. (ingen dato(c)). NIBE. Hentet 29.03, 2019, fra https://www.bits.no/bank/nibe/

Bits AS. (ingen dato(d)). BALTUS 2.0. Hentet 29.03, 2019, fra https://www.bits.no/bank/baltus-2-0/

Bits AS. (ingen dato(e)). BOLS. Hentet 29.03, 2019, fra https://www.bits.no/bank/bols/

Bits AS. (ingen dato(f)). ISO 20022. Hentet 30.03., 2019, fra https://www.bits.no/bank/iso-20022/

Bits AS. (ingen dato(g)). Konto og adresseringsre-gister (KAR). Hentet 14.04, 2019, fra https://www.bits.no/bank/konto-og-adresseringsregister-kar/

Brodsky, Laura & Oakes, Liz. (2017). *Data sharing and open banking*. Hentet fra https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf

Datatilsynet. (2018a). Skytjenester. Hentet 10.05, 2019, fra https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

Datatilsynet. (2018b). Hva er Privacy Shield? Hentet 19.05, 2019, fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/hva-er-privacy-shield/

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner - Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf.

du Toit, Gerard. & Cheris, Aaron. . (2018, 25.09.18). Bank Customers Are Primed And Ready For Amazon. *Forbes*. Hentet fra https://www.forbes.com/sites/baininsights/2018/09/25/bank-customers-are-primed-and-ready-for-amazon/#cd1e42c13fe3

EBA. (2018). *Consultation Paper - EBA draft Guidelines on ICT and security risk managment*. Hentet fra https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf

Eide, Espen. (2017). Vil globale teknologiselskaper konkurrere ut norske banker? *Praktisk økonomi & finans*, *33*(03), 329-331. doi:10.18261/issn.1504-2871-2017-03-03

Elster, Kristian. (2018). Trumps valgrådgivere skryter av skitne triks på skjult kamera. *NRK*. Hentet fra https://www.nrk.no/urix/trumps-valgradgivere-skryter-av-skitne-triks-pa-skjult-kamera-1.13970381

Engen, Ole Andreas, Kruke, Bjørn Ivar, Lindøe, Preben, Olsen, Kjell Harald, Olsen, Odd Einar & Pettersen, Kenneth Arne. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm akademisk.

European Central Bank. (2019). *MANDATE OF THE WORKING GROUP ON A SEPA API ACCESS SCHEME*. Hentet fra

https://www.ecb.europa.eu/paym/retpaym/shared/pdf/Mandate_of_the_working_group_on_a_SEPA_API_access_scheme.pdf?e98a53917c70cd215d2d586adac3b10a.

Evry AS. (2017). *Open Banking Transformation*. Hentet fra https://www.evry.com/globalassets/files/financialservices/final-open-banking-f170214_webb.pdf

Ferguson, Niall. (2008). *The ascent of money : a financial history of the world*. New York: The Penguin Press.

Finans Norge. (2014). Skal vise hva sparebankene står for. Hentet 24.01.19, fra https://www.finansnorge.no/aktuelt/nyheter/2014/09/-skal-vise-hva-sparebankene-star-for/

Finans Norge. (2017). *Beredskap for kontantdistribusjon - høringssvar*. Oslo Hentet fra https://www.regjeringen.no/contentassets/56750b40480d4f4aae3d7e81b8ebce4c/finans_norge1.pdf?uid=Finans_Norge.

Finans Norge. (2019). Nordic Financial CERT: Finansnæringens forsvar mot dataangrep. Hentet 19.05, 2019, fra https://www.finansnorge.no/aktuelt/nyheter/2019/03/nordic-financial-cert-finansnaringens-forsvar-mot-dataangrep/

Finansavtaleloven. (1999). *Lov om finansavtaler og finansoppdrag (LOV-1999-06-25-46)*. Hentet fra https://lovdata.no/dokument/NL/lov/1999-06-25-46.

Finansdepartementet. (2018a). *Finansmarkedsmeldingen 2018* (Meld. St. 14 (2017-2018)). Hentet fra https://www.regjeringen.no/contentassets/82cd2c146891461e9ac8a3aec2a5e6f5/no/pdfs/stm201720180014000dddpdfs.pdf

Finansdepartementet. (2018b). *Nasjonalbudsjettet 2018*. (Meld. St. 1 (2017-2018)). Hentet fra https://www.regjeringen.no/contentassets/6fc0451c5069408791d67ca2fdcc51eb/no/pdfs/stm201720180001000dddpdfs.pdf.

Finansforetaksforskriften. (2017). *Forskrift om finansforetak og finanskonsern (FOR-2016-12-09-1502)*. Hentet fra https://lovdata.no/dokument/SF/forskrift/2016-12-09-1502.

Finansforetaksloven. (2015). *Lov om finansforetak og finanskonsern (LOV-2015-04-10-17)* Hentet fra https://lovdata.no/dokument/NL/lov/2015-04-10-17.

Finanstilsynet. (2017a). *Risiko- og sårbarhetsanalyse (ROS) 2016*. Hentet fra https://www.finanstilsynet.no/contentassets/63187295c2b345f895523e54ee408783/risiko-og-sarbarhetsanalyse-2016.pdf.

Finanstilsynet. (2017b). *Finansielt utsyn 2017*. Hentet fra https://www.finanstilsynet.no/contentassets/93c4406301b747d0879dd80ea5d3deee/finansielt-utsyn-2017.pdf.

Finanstilsynet. (2018). *Risiko- og sårbarhetsanalyse (ROS) 2017*. Hentet fra https://www.finanstilsynet.no/contentassets/b9cb0cab82304c4498a1562a002bafce/risiko--og-sarbarhetsanalyse-2017.pdf.

Finanstilsynet. (2019). *Risiko- og sårbarhetsanalyse 2018*. Hentet fra https://www.finanstilsynet.no/contentassets/a92eb0d064a94bcfa0b8d862936af02e/risiko--og-sarbarhetsanalyse-2018.pdf.

Finanstilsynet & Norges Bank. (2016). *Beredskapsløsninger i betalingssystemet - utkast til høringsnotat*. Oslo Hentet fra https://www.regjeringen.no/contentassets/fafab98e41cf40e3a9a6043d92ebccc3/hoeringsnotat31012017.pdf.

Finanstilsynsloven. (1956). *Lov om tilsynet med finansforetak mv. (LOV-1956-12-07-1)*. Hentet fra https://lovdata.no/dokument/NL/lov/1956-12-07-1.

Gottschalk, Petter. (2013). *Flytting av arbeidsoppgaver til utlandet*. Hentet fra https://www.finansforbundet.no/wp-content/uploads/2017/01/Flytting-av-oppgaver-til-utlandet.pdf

Haare, Harald. (2007). *Clearing and Settlement at Norges Bank – a Historical Review*. (0029-1676). Norges Bank Hentet fra https://static.norges-bank.no/globalassets/upload/english/publications/economic-bulletin/2007-04/clearing-and-settlement.pdf?v=03/09/2017122215&ft=.pdf.

Haare, Harald & Solheim, Jon A. (2011). *Utviklingen av det norske betalingssystemet i perioden 1945-2010, med særlig vekt på Norges Banks rolle*. (0802-7188

978-82-7553-631-8). Norges Bank Hentet fra https://static.norges-bank.no/contentassets/0835b118822d4c6b886e8aa407ba03b1/skriftserie_44.pdf?v=03/09/2017123444&ft=.pdf.

Hollnagel, Erik. (2004). *Barriers and accident prevention*. Aldershot Hampshire: Ashgate Publishing Company.

Honningsvåg, Christina. (2018, 06.09.18). Betale med mobilen, klokka eller nettbrettet? Hentet 23.03, 2019, fra https://www.dinside.no/data/betale-med-mobilen-klokka-eller-nettbrettet/70150648

Hopland, Sindre. (2018, 30.10.18). Google Pay lanseres i Norge. Hentet fra https://e24.no/naeringsliv/google/google-pay-lanseres-i-norge/24475843

IRGC. (2018). *Guidelines for the Governance of Systemic Risks*. Hentet fra Lausanne: https://www.irgc.org/wp-content/uploads/2018/09/IRGC-2018.-IRGC-Guidelines-for-the-governance-of-systemic-risks.pdf

Justis- og beredskapsdepartementet. (2012). *Samfunnssikkerhet*. (Meld. St. 29 (2011-2012)). Hentet fra https://www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf.

Justis- og beredskapsdepartementet. (2016). *Risiko i et trygt samfunn*. (Meld. St. 10 (2016-2017)). Hentet fra https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf.

Justis- og politidepartmentet. (2002). *Samfunnssikkerhet - Veien til et mindre sårbart samfunn*. (Meld. St nr. 17 (2001-2002)). Hentet fra https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf.

Kjellén, Urban. (2000). *Prevention of accidents through experience feedback*. London: Taylor & Francis.

Knudsen, Camilla. (2019, 02.04.19). DNB ser tøff konkurranse fra Apple, Google og Facebook. *E24*. Hentet fra https://e24.no/boers-og-finans/bank/dnb-ser-toeff-konkurranse-fra-apple-google-og-facebook/24594568

Kvale, Steinar. (1997). *Det kvalitative forskningsintervju* (Tone Anderssen & Johan Rygge, overs.). Oslo: Ad notam Gyldendal.

Langbraaten, Nina. (2012). Nye betalingsmåter. *Penger og Kreditt, 2012*(1), 14-21.

Larsen, Marcus M., Manning, Stephan & Pedersen, Torben. (2013). Uncovering the hidden costs of offshoring: The interplay of complexity, organizational design, and experience. *Strategic Management Journal, 34*(5), 533-552. doi:10.1002/smj.2023

Lind, Øyvind Andreas. (2016). Smitte mellom banker – Systemrisiko som følge av bankenes sammenkobling: Norges Bank.

Lonsdale, Chris & Cox, Andrew. (2000). The historical development of outsourcing: the latest fad? *Industrial management & data systems, 100*(9), 444-450.

Nasjonal Sikkerhetsmyndighet. (2015). *Veileder i sikkerhetsstyring*. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf.

Nordea. (2017). Nå kan du betale regninger via Facebook Messenger. Hentet 24.01.19, fra https://www.nordea.com/no/presse-og-nyheter/nyheter-og-pressemeldinger/press-releases/2017/11-29-08h46-na-kan-du-betale-regninger-via-facebook-messenger.html

Nordea. (ingen dato). Apple Pay er her. Hentet 24.01.19, fra https://www.nordea.no/privat/vare-produkter/nettbank-og-mobilbank/apple-pay.html

Norges Bank. (2004). *Årsrapport om betalingsformidling 2003*. (1503-8610). Oslo: Norges Bank Hentet fra https://static.norges-bank.no/contentassets/cb79ed5f62164c13b825f4147c7d5f19/betaling-hele-2003.pdf?v=03/09/2017122052&ft=.pdf.

Norges Bank. (2014). *Kostnader i det norske betalingssystemet*. (1894-0269

978-82-7553-830-5). Oslo Hentet fra https://static.norges-bank.no/contentassets/c6ed2ec861034f47afb5ea233363a5d3/norges_bank_memo_5_2014.pdf?v=03/09/2017123516&ft=.pdf.

Norges Bank. (2016a). *Det Norske finansielle systemet : en oversikt*. (2535-3993). Oslo: Norges bank.

Norges Bank. (2016b). *Norges Bank Memo - Det norske finansielle systemet*. Hentet fra https://static.norges-bank.no/contentassets/32c65e2235634ea4a366e306af62e7e9/nb_memo_2_2016.pdf?v.

Norges Bank. (2017). *Finansiell infrastruktur 2017*. Oslo Hentet fra https://static.norges-bank.no/contentassets/0af5e6ca88d54c7ca6ab9cd8b44257c8/finansiell_infrastruktur_2017.pdf?v=05/18/2017145640&ft=.pdf.

Norges Bank. (2018a). *Finansiell infrastruktur 2018*. Hentet fra https://static.norges-bank.no/contentassets/234480bf59cf4c02a5b2f7b18c97008f/finansiell_infrastruktur_2018.pdf?v=05/25/2018091305&ft=.pdf

Norges Bank. (2018b). *Det Norske finansielle systemet, en oversikt*. Oslo Hentet fra https://static.norges-bank.no/contentassets/d8039ff2c8a9438c9400132c46c241e1/dnfs_2018.pdf?v=07/03/2018125144&ft=.pdf.

Norges Bank. (2018c). *Kunderetta betalingsformidling 2017*. (1894-0269

978-82-8379-035-1). Norges Bank Hentet fra https://static.norges-bank.no/contentassets/acf2fe440bc6483393bda6d66acc29fa/nb_memo_2_18.pdf?v=05/24/2018084221&ft=.pdf.

Norges Bank. (2018d). *Finansiell stabilitet - Sårbarhet og risiko*. Hentet fra https://static.norges-bank.no/contentassets/1afe861c5f1c43afaf61fb57082e7c7a/fs2018_rapport.pdf?v=11/23/2018133919&ft=.pdf.

Norges Bank. (2019). *Finansiell Infrastruktur 2019*. Hentet fra https://static.norges-bank.no/contentassets/8c65f4c19bcb49be9e49985629b41968/finansiell_infrastruktur2019.pdf?v=05/23/2019160305&ft=.pdf.

NOU 2000:24. (2000). *Et sårbart samfunn*. Oslo Hentet fra https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf.

NOU 2015:13. (2015). *Digital sårbarhet – Sikkert samfunn*. Oslo: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf.

NOU 2016:19. (2016). *Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Hentet fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf.

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet* Oslo: Justis- og beredskapsdepartementet Hentet fra https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf.

Payr. (ingen dato). Full oversikt på et øyeblikk. Hentet 19.03, 2019, fra https://www.payr.no/full-oversikt-med-payr

Perrow, Charles. (1999). *Normal accidents : living with high-risk technologies*. Princeton, New Jersey: Princeton University Press.

Porter, Michael E. (1985). *Competitive advantage : creating and sustaining superior performance*. New York: Free Press.

Power, Mark J., Desouza, Kevin C. & Bonifazi, Carlo. (2006). *The outsourcing handbook : how to implement a successful outsourcing process*. London: Kogan Page.

PSD2. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives*

2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC Hentet fra https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

Reason, James. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Renn, Ortwin. (2008). *Risk governance : coping with uncertainty in a complex world*. London: Earthscan.

Renn, Ortwin, Klinke, Andreas & Asselt, Marjolein. (2011). Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis. *A Journal of the Human Environment, 40*(2), 231-246. doi:10.1007/s13280-010-0134-0

Ringdal, Kristen. (2013). *Enhet og mangfold : samfunnsvitenskapelig forskning og kvantitativ metode* (3. utg. utg.). Bergen: Fagbokforl.

Solheim, Jon A. & Strømme, Helge. (2003). *Modernisering og utkontraktering av Norges Banks oppgjørssystem*. (0332-5598). Norges Bank Hentet fra https://static.norges-bank.no/globalassets/upload/publikasjoner/penger_og_kreditt/2003-04/nbo.pdf.

SWIFT. (ingen dato.). Introduction to SWIFT. fra https://www.swift.com/about-us/discover-swift

Taleb, Nassim Nicholas. (2007). *The black swan : the impact of the highly improbable*. London: Allen Lane.

Thagaard, Tove. (2018). *Systematikk og innlevelse : en innføring i kvalitative metoder* (5. utg. utg.). Bergen: Fagbokforl.

The Guardian. (2017, 11.10.17). Personal details of almost 700,000 Britons hacked in cyber-attack. *The Guardian*. Hentet fra https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack

Tjora, Aksel Hagen. (2012). *Kvalitative forskningsmetoder i praksis* (2. utg. utg.). Oslo: Gyldendal akademisk.

Vedlegg

Vedlegg 1, informasjonsskriv til informanter.

Informasjonsskriv intervju og intervjuguide.

Bakgrunnsinformasjon.

Intervjuet er knyttet til en masteroppgave i samfunnssikkerhet og risikostyring ved Universitetet i Stavanger. Om ytterligere informasjon er ønskelig, bes det om å ta kontakt med intervjuer.

Andreas Schei Andersen vil gjennomføre intervjuet.

Vedlagt ligger det også et dokument med begrepsavklaring for å ha en enstydig begrepsforståelse.

Om det er spørsmål knyttet til dette så tas dette med intervjuer.

Anonymitet.

Dere som blir intervjuet vil ha full anonymitet i oppgaven. Det vil ikke bli nevnt navn, kjønn, grad, stilling eller avdeling. Hver informant vil få et nummer som kun oppgavens medlemmer vil kjenne til. Dere kan når som helst trekke dere fra studien ved å kontakte meg.

Det vil bli forespurt om å benytte seg av båndopptaker under intervjuet. Årsaken til dette er for å få dokumentert så mye informasjon som mulig. Dersom du på et tidspunkt skal formidle informasjon du vil ha taushetsbelagt stoppes opptaket og informasjonen vil ikke bli brukt i oppgaven.

Ved bruk av båndopptaker vil intervjuet bli transkribert, dette sendes over til informantene for validering. Er du feilsitert, noe som kommer frem feil eller lignende, ta kontakt med intervjuer.

Er det behov for ytterligere informasjon ta kontakt med intervjuer.

Andreas Schei Andersen kan nås på:

Email: [redacted] / [redacted]

Telefon: [redacted]

Vedlegg 2, intervjuguide banker

Intervjuguide bank

Innledningsspørsmål:

Hva er din rolle i organisasjonen?

Hvilken rolle har din organisasjon i den norske betalingsformidlingen?

Hva anser du som kjerneoppgavene til et finansielt system?

Hvordan vil du beskrive det norske betalingssystemet?

Dybdespørsmål:

1. Hvilke sårbarheter mener du finnes i betalingsformidlingen i Norge?
2. Hvilke deler av verdikjeden for betalingsformidling anser du som utsatt for fragmentering som en følge av PSD2 og/eller outsourcing?
3. Hvordan blir deres ansvar for sikker betalingsformidling påvirket av open banking?
4. Hvordan vurderer du at outsourcing/tjenestutsetting kan påvirke sikkerheten knyttet til betalingsformidling?
5. Hvordan jobber du og din virksomhet i å bevare sikkerhet i møte med nye aktørers inntog?
6. Hvordan blir arbeidet med samfunnssikkerhet og beredskap preget av nye aktører som ikke nødvendigvis er direkte underlagt norske regler?

Avslutningsvis:

Har du noen bemerkninger eller noe du ikke fikk formidlet?

Noe du vil legge til?

Vedlegg 3, intervjuguide IT-selskap

Intervjuguide IT-selskap

Innledningsspørsmål:

Hva er din rolle i organisasjonen?

Hvilken rolle har din organisasjon i den norske betalingsformidlingen?

Hva anser du som kjerneoppgavene til et finansielt system?

Hvordan vil du beskrive det norske betalingssystemet?

Dybdespørsmål:

1. Hvilke sårbarheter mener du finnes i betalingsformidlingen i Norge?
2. Hvilke deler av verdikjeden for betalingsformidling anser du som utsatt for fragmentering som en følge av PSD2?
3. Hvordan påvirker outsourcing fokus knyttet til sikkerhet i organisasjonen?
4. Hvilken innvirkning vil open banking ha på sikkerheten i den norske betalingsformidlingen?
5. Hvilke konsekvenser kan et bredere spekter av aktører i betalingsformidlingen ha for samfunnssikkerheten i Norge?
6. Hvordan arbeider du og din virksomhet for å opprettholde tilstrekkelig sikkerhet i deres løsninger, både nye og gamle?

Avslutningsvis:

Har du noen bemerkninger eller noe du ikke fikk formidlet?

Noe du vil legge til?

Vedlegg 4, intervjuguide fintech-selskap

Intervjuguide fintech

Innledningsspørsmål:

Hva er din rolle i organisasjonen?

Hvilken rolle har din organisasjon i den norske betalingsformidlingen?

Hva anser du som kjerneoppgavene til et finansielt system?

Hvordan vil du beskrive det norske betalingssystemet?

Dybdespørsmål:

1. Hva mener du PSD2/open banking bidrar til i betalingslandskapet?
2. Hvilke deler av verdikjeden for betalingstjenester sikter dere inn på?
3. Hva mener du kjennetegner nye aktører inn i betalingsformidlingen?
4. Hvordan jobber dere inn mot banker for tilgjengeliggjøring av tjenester?
5. Hva knyttet til deres tjenester er viktig å sikre?
6. Hvordan jobber dere med sikkerhet i deres løsninger?

Avslutningsvis:

Har du noen bemerkninger eller noe du ikke fikk formidlet?

Noe du vil legge til?

Vedlegg 5, intervjuguide myndigheter

Intervjuguide myndigheter

Innledningsspørsmål:

Hva er din rolle i organisasjonen?

Hvilken rolle har din organisasjon i den norske betalingsformidlingen?

Hva anser du som kjerneoppgavene til et finansielt system?

Hvordan vil du beskrive det norske betalingssystemet?

Dybdespørsmål:

1. Hvilke sårbarheter finnes i betalingsformidlingen i Norge?
2. Hvordan vil du vurdere beredskapen knyttet til elektroniske betalingstjenester?
3. Hvordan foregår sikkerhetsarbeidet i betalingsformidling og hvordan bistår dere?
4. Hvilke deler av verdikjeden for betalingsformidling anser du som utsatt for fragmentering som en følge av PSD2/open banking?
5. Hvordan påvirker outsourcing sikkerhet i den norske betalingsformidlingen?
6. Hvilke konsekvenser kan et bredere spekter av aktører i betalingsformidlingen ha for samfunnssikkerheten i Norge?

Avslutningsvis:

Har du noen bemerkninger eller noe du ikke fikk formidlet?

Noe du vil legge til?

Vedlegg 6, historisk utvikling av norsk bankinfrastruktur

Tilgjengeliggjøring av elektroniske betalingstjenester

Digitalisering av betalingstjenester i Norge har vært preget av utvikling innen EDB, datamaskinen og i senere tid mobil- og smarttelefonen. Utviklingen tradisjonelt sett har ligget i initiativ fra bankene selv, som har opprettet datasentraler. Datasentralene har vært sentrale i utviklingen av elektroniske betalingstjenester og er fortsatt i dag sentrale i utviklingen av moderne digitale betalingstjenester. Et av disse samarbeidene var etableringen av datasentralen Fellesdata som fant sted i 1965, dette var et samarbeid mellom Fellesbanken A/S, Sparebankene og Sparebankforeningen. Fellesdata var sentrale i utviklingen av de første minibankene som kom til Norge (Haare & Solheim, 2011, s. 35,58). Årsaken til opprettelsen var et ønske om tettere samarbeid innen EDB. Opprettelsen av BBS, Vestdata og Norddata også et sentrale steg i denne utviklingen. Samarbeidet rund Fellesdata gjorde det mulig for sparebankene å introdusere bankkort til sine kunder, Fellesdata var sentrale i denne utviklingen og minibanker (Finans Norge, 2014). Det var dog ikke norske banker som var først ute med å tilby betalingskort til det norske markedet.

Kjøpekort i regi av Bokreditt A/S var i 1957 først ute med å tilby brukerne betalingskort, kjøpekortet kunne bare benyttes i Norge. Banknæringen tok ikke særlig del i denne utviklingen (Haare & Solheim, 2011, s. 55-56). Bankene påbegynte arbeidet med å introdusere bankkortløsninger til sine brukere, først gjennom et samarbeid med Bokreditt Kjøpekort AS som allerede var kjent med betalingskort. En avtale kom aldri på plass så bankene forsøkte da å etablere et eget system. Norges Bank satte derimot en brems på prosjektet da de heller ville ha et utvalg til å redegjøre for usikkerhetene knyttet til implementering av bankkort (ibid.). I påvente av tillatelse til å introdusere bankkort til det norske markedet opprettet en rekke banker selskapet Visa AS i 1977. Kredittkortet skulle benyttes til transaksjoner utenlands (ibid., s. 57). Andre internasjonale kredittkortselskap hadde allerede blitt introdusert til det norske markedet på denne tiden, Diners Club fikk sin tillatelse til å drive allerede i 1968 mens flere sparebanker inngikk i en samarbeid med Eurocard International. Noe som kulminerte i opprettelsen av Eurocard Norge i 1972 (ibid.). Norske betalingskort, i regi av bankene, var derfor på etterskudd sammenliknet med de norske og internasjonale kredittaktørene. De første kortene i regi av norske banker ble introdusert i forbindelse med minibankene. Datasentralen Fellesdata var sentral i utviklingen og de første minibankene ble utplassert i Norge i 1977, i starten var minibankene knyttet til brukerkontoer i minibankene utstedt av banken.

I 1984 ble det derimot introdusert kort for nasjonal bruk for både butikkterminaler og minibanker, samt i kombinasjon med debetkort med VISA-løsning, disse ble utstyrt med en magnetstripe som avleser (Haare & Solheim, 2011, s. 27-28). Teknologien var derimot ikke fullt utviklet og derfor var forelå det ikke løsninger som tillot forskjellige kort i forskjellige terminaler. Det var dog ulike bankforeninger som gikk inn i, stor grad bilaterale, samarbeid om felles betalingsløsninger også kjent som EFTPOS-system. Samordningen av EFTPOS-systemene har siden blitt samlet i BankAxept. Det største hinderet i samordning av betalingsløsninger kan i all hovedsak stilles til det fragmenterte aktørbilde hvor forretningsbanker, sparebanker og Postbanken alle tidligere benyttet ulike format for sine betalingstjenester. Dette igjen hadde medført ulik prissetting mellom de ulike systemene og tjenestene, noe som innvirket på interbanksystemet (ibid., s. 17). I 1991 ble det introdusert en felles betalingsløsning, dette var en utvidelse av felles EFTPOS-samarbeid. Samordningen av betalingstjenester fikk navnet BankAxept og ble driftet av BankAxept A/S (Haare & Solheim, 2011, s. 29). Kortsystemet ble tatt i bruk fra 1993, teknologien var basert på magnetstripe. BankAxept var et viktig steg mot en felles operasjonell infrastruktur i norsk betalingsformidling, av denne årsak har BankAxept relevans for backend. En kan derfor vurdere BankAxept som grensende mellom både front- og backend. Denne tjenesten ble i 2005 utvidet til å gjelde betalinger over nett, da gjennom BankAxess (ibid.).

Girotjenester i Norge har vært tilstede siden 1943, hvor postgiro ble etablert som det første systemet for kontobasert betalingsformidling. Tjenesten var primært knyttet opp mot offentlige virksomheter, men også private organisasjoner (Haare & Solheim, 2011, s. 60). Bankene introduserte et lignende tilbud, bankgiro, i 1946. Målet for bankene var å utvikle bedre og billigere tjenester for kundene samt skape en motvekt til postgiro (ibid.). Bruk av to giroløsninger uten samordning viste seg å være dyrt og ineffektivt. Så det ble påbegynt samtaler mellom Bankforeningene og Postverket i forsøk på å samordne de to girosystemenene allerede på slutten av 1950-tallet (ibid., s. 61). Samtalene foregikk parallelt med en form for konkurranse og teknologisk utvikling for begge parter. Denne stagneringen viste seg å være uhensiktsmessig for samtlige parter berørt av manglende samordning av disse girosystemene. På slutten av 1980-tallet intensifierte derimot disse diskusjonene med Norges Bank som en sentral part (ibid., s. 121). På 1990-tallet etter Postgiro og Norges Postbank fusjonerte til Postbanken, som da opererte som andre banker presenterte muligheten for samordning mellom post- og bankgiro. I 1996 ble en felles giroblankett innført (ibid., s. 128). Innunder denne samordningen ble også AvtaleGiro og AutoGiro innlemmet, dette var

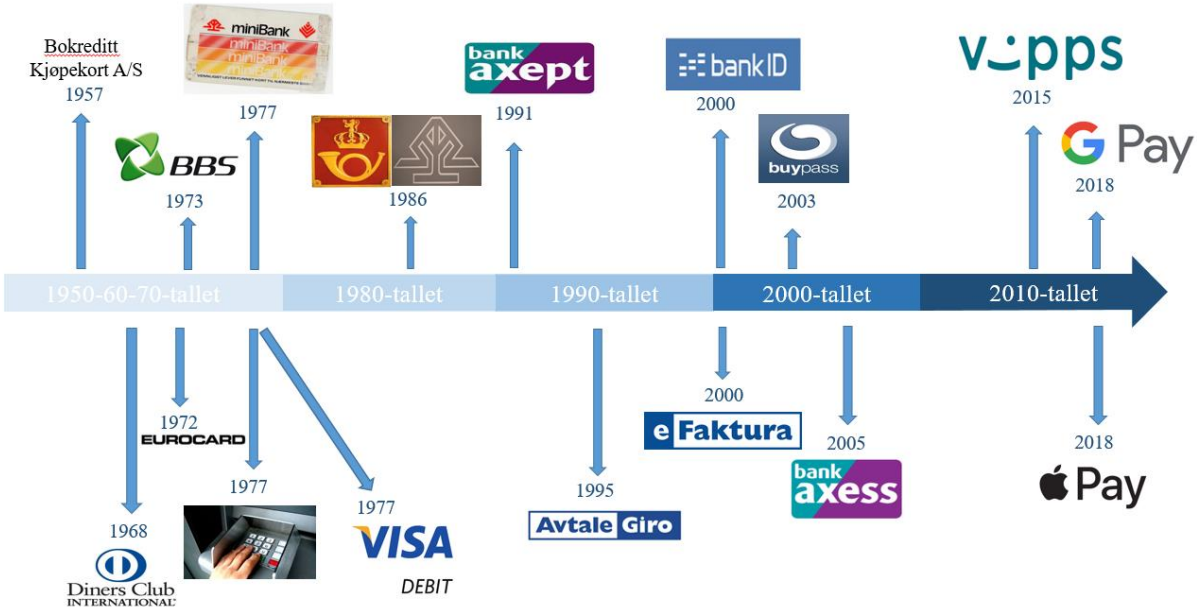
automatiske gireringer mellom konti i ulike banker. Brukere kunne nå gå inn i avtaler om dette med betalingsfordrer for betaling av regninger og overføringer (ibid.). Dette var en digitalisert versjon av den allerede eksisterende autogiro-ordningen, AvtaleGiro erstattet denne ordningen (ibid., s. 137).

Datamaskinens økende integrasjon i samfunnet på 1980- og 1990-tallet presenterte en rekke muligheter innen betalingsformidling og –tjenester. En utvikling som belaget seg på økende integrering av EKOM i det norske samfunnet var bruk av e-penger. E-penger ble introdusert som en betalingsmåte i Norge i 2003 da fire e-pengeforetak, deriblant BuyPass, fikk konsesjon til å drive sitt virke (Norges Bank, 2004, s. 31). E-penger var allerede tilstede i andre europeiske land på denne tiden, trenden begynte allerede på 1990-tallet. Norske banker og myndigheter så derimot på 1990-tallet på dette med litt pessimisme da det var usikkerhet knyttet til hvordan dette ville innvirke på den eksisterende betalingsinfrastrukturen, særlig med tanke på bruk og utbredelse av pengekort (Haare & Solheim, 2011, s. 142-143). Betalinger ved bruk av e-penger er globale i den forstand at de er grensekryssende uten en sentralbank eller myndighet som utsteder av betalingsmiddelet. Utstederen er i denne sammenheng også tilbyderen av tjenesten, eksempler på dette er Revolut og PayPal som er to store aktører med samarbeidsavtaler med en rekke banker.

En annen betalingsløsning som kunne presenteres til det norske markedet grunnet den økende digitaliseringen var banktjenester via internett. Nettbank fikk på 1990-tallet økt fokus i Norge, den første norske nettbanken ble lansert i 1996 og innen 1999 hadde så å si alle banker tjenester tilgjengelig på nettbank (Haare & Solheim, 2011, s. 139). Datasentralene var sentrale i utviklingen av disse tjenestene som tjente samme funksjon som tidligere hadde blitt introdusert, men var mer brukervennlig da dette kunne gjøres på PC-skjermen (ibid.). Til tross for digitaliseringen av banktjenester var fortsatt netthandelen veldig liten. En tilbud gitt til nettbank-brukerne var elektronisk presentasjon av fakturaer i nettbank. eFaktura ble utviklet av BBS og EDB Fellesdata i samarbeid med bankene og en rekke foretak. Løsningen ga betaler fakturainformasjonen i nettbanken og betalingskravet kunne godkjennes elektronisk av betaler (ibid., s. 208). Noe som underbygde denne EKOM-trenden og ivaretakelse av sikkerhet var Bank ID. BankID ble etablert i 2000 som en base for at bankene skulle kunne utvikle elektroniske løsninger med tilstrekkelig sikkerhet (Haare & Solheim, 2011, s. 30).

Mobiltelefonens inntog presenterte også flere muligheter for betalingstjenester og –formidling for bankene (Haare & Solheim, 2011, s. 209). I 1994 ble tjenestene Telegiro og Telebank tatt i bruk, ved bruk av telefonen kunne en da sjekke saldo, betale regninger og overføre mellom

egne kontoer (ibid., s. 139). Videre ble også tjenester andre tjenester introdusert, disse var knyttet opp mot SMS og SIM-kortet til mobiltelefonen. Banktjenester som å sjekke saldo og betalingstjenester som kunne belastes det forhåndsbetalte kontantkortet, var noen av disse (ibid., s. 209). Betalingstjenester og -formidling på mobil ble mer aktuelt og fikk utbredt potensial ved utbredelsen av smarttelefonen i Norge. En har siden utbredelsen av smarttelefonen sett inntoget av nye tjenester knyttet til betaling og bank som mobilbank, mCash, MobilePay og VIPPS er noen av disse. Smarttelefonen og de tilhørende tjenestene knyttet til det har endret konteksten for tilgangen på banktjenester.



Figur 15, tidslinje for sentrale endringer for betalingstjenester

Av figur 2 kan en se de sentrale hendelsene for frontend-løsninger mot markedet og forbrukeren. Til tross for at begivenhetene ikke er store på 1980-tallet så er det i dette tiåret digitalisering virkelig setter fart knyttet til løsningene mot brukerne. Tegnene en ser på nettopp denne digitaliseringen ser en ved løsninger som nettbank, eFaktura og BankAxess. BuyPass, PayPal, Apple Pay, Google Pay viser hvordan betalingsløsningene blir i større grad verdensomspennende enn tidligere. Google og Apple Pay er brukt som en illustrasjon på et mer globalisert bilde i betalingsformidling i det norske samfunnet. Utenom disse aktørene er det en rekke andre internasjonale selskap som utfordrer de norske bankenes tilbud på betalingstjenester. En kan også identifisere et mer fragmentert aktørbilde av tilbydere av betalingstjenestene enn tidligere. Tidligere har utvikling og tilbud av betalingstjenestene i Norge vært nesten forbeholdt den norske banknæringen, dog med noen forbehold, hvor det nå

er et mye mer globalisert og fragmentert aktørbilde som preger utviklingen av betalingstjenester.

Utvikling av interbanksystemet

Norges Bank har fungert som oppgjørsbank i Norge siden 1898 (Haare & Solheim, 2011, s. 34). Endringene i interbanksystemet har vært store i dette tidsrommet, de største endringene har dog funnet sted etter 1960-tallet (Haare, 2007, s. 153). Økende digitalisering av systemer og fremveksten av datasentraler var drivkrefter i interbanksystemet frem til 1980-årene. Fra midten av 1980-årene og utover begynte arbeidet med samordning av de ulike datasentralene for å operasjonalisere en felles samordning for interbanksystemet. Dette kulminerte i opprettelsen av Norwegian Interbank Clearing System også kjent som NICS på 1990-tallet og dets tette tilknytning til og Norges Bank Oppgjørssystem kjent som, NBO.

Allerede fra 1950-tallet ble samarbeid innen EDB aktuelt for bankene grunnet de høye kostnadene knyttet bruk av dette. Opprettelse av datasentraler som A/S Integrert Databehandling nå kjent som IDA, Fellesdata, Norddata og Vestdata – senere NOVIT., var en reaksjon bankene hadde for dette (Haare & Solheim, 2011, s. 63-64). IDA og Fellesdata var sentrale i utvikling og standardisering for økt effektivitet i avregning mellom bankene. Sentralt i utviklingen var samordning og bruk av EDB. En konsekvens av standardiseringen var påbegynnelsen av det vi i dag kjenner som kontonummer. En sentral del i å kunne benytte seg av EDB-teknologi var at det forelå et felles struktur for kontosystemer, dette ble gjort ved bruk av en ellevesiffer lang kode. Fire første siffer viste til hvilken institusjon kontoen var, de neste seks var for kundekontiene internt i institusjonen og det siste sifferet var kontrollsiffer (ibid.). Opprettelsen av BBS er også sentralt innen denne generelle utviklingen grunnet deres sentrale rolle innen avregning av bankgiro og oppgjør mot Norges Bank (ibid., s. 67). Datasentralene var sentrale i avregningen av sjekker mellom bankene, IDA og Fellesdata var de mest sentrale aktørene her. Avregningen ble gjort av enten IDA eller Fellesdata, datasentralene benyttet seg av nyere EDB-teknologi for denne avlesingen (Haare & Solheim, 2011, s. 68). Senere har datasentralene fusjonert sammen, dette har i så måte også økt graden av samordning på betalingstjenestene som ble tilbudt av bankene. Datasentralene var starten på samordning mellom bankene, til tross for at det fantes flere ulike sentraler var disse opprettet i samarbeid mellom

Oppgjørsrisiko for bankene kom i fokus på slutten av 1980-tallet, gjennom internasjonale organisasjoner og etter Norion Bank ble insolvens og satt under offentlig administrasjon.

Gjennom 1990-tallet ble oppgjørssystemet oppdatert til å bli ett system hvor risikoen ble redusert, samt at effektiviteten i oppgjørene økte (Haare & Solheim, 2011, s. 147). Siden 1999 og oppstarten av det nye oppgjørssystemet NBO fikk Norge et RTGS-system, sammen med NICS utgjorde dette et moderne avregning- og oppgjørssystem (ibid., s. 150). NICS ble utviklet av BBS på 1990-tallet, som et felles avregnings- og likviditetsinformasjonsystem. Etableringen av NICS medførte at bankene måtte følge, styre og oppdatere sin likviditet gjennom dagen. Operatørkontoret NICS kom i 2000 og har konsesjonen og operatøransvaret for interbanksystemet NICS. Driften ble utkontraktert til BBS Infrastruktur AS nå NETS Norge Infrastruktur AS (Haare & Solheim, 2011, s. 37). Avregning mellom bankene var tidligere gjennom system som ikke var felles, gjerne bilateralt med hverandre via ulike datasentraler (ibid., s. 35).

Samordning og standarder

I løpet av 1990-tallet så ble datameldingsstandarder i økende grad benyttet for å standardisere betalingstjenestene og kommunikasjon mellom bankene. Standardiseringsarbeidet har ikke vært helt uten internasjonal innflytelse da EF/EU, SWIFT og andre organisasjoner har hatt innvirkning på standardene implementert i Norge.

En av de første standardene som ble implementert med formål å forenkle kommunikasjon mellom fordrer og betaler var KID. KID-nummerering ble introdusert i 1973 av BBS som et ledd i den generelle EDB-utviklingen hvor det i større grad skulle digitaliseres (Haare & Solheim, 2011, s. 69). KID-nummeret ble introdusert for å identifisere kunden og fakturaen som ble betalt, uavhengig av hvem som sto som betaler (ibid.).

Norges Bank ble medlem av SWIFT i 1974, dette var et langt steg mot både effektivisering og digitalisering av pengeoverføringer ovenfor utlandet (Haare & Solheim, 2011, s. 71). Dette steget knyttet også det norske bankvesenet inn i et stort internasjonalt nettverk. Deltagelsen i dette nettverket stiller en rekke krav til aktørene med henhold til sikkerhetskrav og standardisering (ibid., s. 72). SWIFT benyttes også til store bruttotransaksjoner innenlands som må gjøres i realtid, disse gjøres opp gjennom avregningssystemet NICS.

BOLS, Bankenes On-Line Standard, ble utviklet og lenge brukt for kommunikasjon mellom bankene. Løsningen ble tenkt erstattet av den norske EDIFACT standarden NIBE, men BOLS er fortsatt benyttet i dag (Bits AS, ingen dato(e)).

Internasjonale standarder som EDIFACT ble benyttet til kommunikasjon mellom bankene. Standardiseringsarbeidet kom på tidlig 1990-tallet til Norge, preget av internasjonale trender og særlig fra EF/EU og til dels også FN (Haare & Solheim, 2011, s. 29). Electronic Data Exchange for Administration, Commerce and Transport også kjent som EDIFACT er et internasjonalt regelverk for standarder i informasjonsutveksling mellom datamaskiner. Arbeidet med implementeringen av en slik standard kunne ha vesentlige samfunnsøkonomiske gevinster, ettersom informasjon kunne formidles elektronisk heller enn på papir (ibid., s. 164). Den nye standarden skulle erstatte den eksisterende kommunikasjonsstandarden for interbank-kommunikasjon BOLS. Dette var et stort steg i utviklingen av en norsk interbankstandard. Norsk interbank standard-EDIFACT også kjent som NIBE, var et initiativ for å utvikle en norsk EDIFACT standard, NIBE ble implementert som interbankstandard i 1998 (ibid., s. 165).

BALTUS, BAnkenes on-Line TransaksjonsUtvekslingsSystem, var et system som gjorde det mulig å gjøre dekningskontroll av konti i andre banker. Systemet ble tatt i bruk i 1986, fra 1989 gjaldt det også minibanker og terminaler (Haare & Solheim, 2011, s. 116). Systemet er siden blitt oppgradert til BALTUS 2.0 (Bits AS, ingen dato(d)).