Er det faktisk motstrid mellom PSD2 og AMLD4 for fullmaktforetaks anti-hvitvaskingsplikter?

En evaluering og rettspolitiske betraktninger.

Kandidatnummer: 245

Antall ord: 13 490

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

7. juni, 2021

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Innovasjon, utvikling og digitalisering har preget betalingstjenester i lang tid. Etter at de første minibankautomatene kom i 1967, har betalingstjenestetilbyderne skrittvis digitalisert sin virksomhet.[1] I dag er finansindustrien en av pådriverne bak den digitale utviklingen og blant de største kundene av digitale tjenester.[2]

Historisk har betalingstjenester primært blitt tilbudt av tradisjonelle banker i Europa, og i 2017 hadde 96,4% av befolkningen i Eurosonen kundeforhold til en bank.[3] Disse bankene har i stor grad vært premissleverandører for innovasjonen, utviklingen og digitaliseringen av den europeiske betalingstjenestenæringen. Konsekvensen har vært at initiativene har blitt begrenset til digitalisering og automatisering internt hos den enkelte aktør, noe som har hevet heller enn senket, terskelen for nye aktører på grunn av begrenset og dyr tilgang på informasjon og teknologi.[4]

Et velfungerende indre marked for produkter og tjenester, er avhengig av et effektivt marked for betalingstjenester. I mange europeiske land dominerer to internasjonale kortnettverk markedet, samtidig som færre enn 4 av 10 europeere har kredittkort.[5] Store ulikheter i tilgangen på betalingstjenester forpurrer unionens kongstanke om tett markedsintegrasjon og fri flyt av varer og tjenester.

Med dette som bakteppe ble Payment Services Directive (PSD1) lansert.[6] Formålet med PSD1 var å fremme konkurransen i markedet for betalingstjenester. Ved å harmonisere regelverket i EØS-området, skulle man skape et felles indre marked for betalingstjenester. Slik skulle det bli mer attraktivt og enklere for nye tilbydere av betalingstjenester å entre markedet.

I 2015 kom Revised Payment Services Directive (PSD2).[7] PSD2 videreførte formålene i PSD1: harmonisere regelverket for europeiske tilbydere av betalingstjenester for å styrke innovasjons- og konkurranseevnen, og sikre forbrukerrettighetene.

[1] Arner, Barberis, Buckley (2016), s. 1274
[2] Arner, Barberis, Buckley (2016), s. 1275
[3] Ehrmann & Ampudia (2017)
[4] Nicoletti (2017), s. 10-11
[5] de Best (2020); Saltkjel (2019)
[6] Directive 2007/64/EC
[7] Directive (EU) 2015/2366

Samme år kom Fourth Anti-Money Laundering Directive (AMLD4).[8] AMLD4 var på samme måte en videreutvikling av regelverket i Third Anti-Money Laundering (AMLD3). Begge direktivene videreførte formålet om å forhindre europeiske aktører å bli misbrukt til hvitvasking.[9] For å oppnå formålet, pålegger AMLD4 en rekke aktørgrupper, inkludert betalingsinstitusjoner, en mengde plikter for å hindre at virksomheten deres blir misbrukt til hvitvasking eller terrorfinansiering gjennom kundeforhold og transaksjoner.

Nytt i PSD2 var en ny gruppe betalingsforetak: fullmaktforetak.

Det er to typer fullmaktforetak. Den ene er betalingsfullmektiger som på en kontoeiers forespørsel, kan igangsette overføringer fra en betalingskonto.[10] Den andre er opplysningsfullmektiger som på en kontoeiers forespørsel, kan hente ut kontohistorikk.[11]

Fullmaktforetakene skiller seg fra andre betalingsforetak ved at de forutsetter kontoeierskap hos et kontotilbydende betalingsforetak. Fullmaktforetak verken mottar, sender eller holder kundemidler.

Fullmaktforetak som kun er fullmaktforetak, berører ganske enkelt ikke, på noe tidspunkt, kundemidler. En praktisk konsekvens av dette, er at fullmaktforetakene kun kan være involvert før en transaksjon gjennomføres, eller etter den er gjennomført, men aldri i selve utførelsen. Dette er også årsaken til at fullmaktforetak også omtales som tredjeparter.[12]

PSD2 og AMLD4 ble utarbeidet parallelt, med en intensjon fra lovgiver om å utarbeide et sammenhengende regelverk på tvers av direktivene. Et spørsmål er likevel om det finnes en faktisk motstrid mellom direktivene når det gjelder fullmaktforetakene.

Virksomheter som kun har konsesjon som fullmaktforetak, har ingen eierskap i betalingstjenesteinfrastruktur og har aldri kontakt med kundemidler. Slik er de også avhengig av at kundene allerede har et kundeforhold til en kontotilbyder.

Kontoeier må altså forholde seg til minst to aktører for å kunne benytte betalingstjenestene til et betalingsforetak som kun er fullmaktforetak: tilbyderen av fullmakttjenesten og kontotilbyder. En betaler, en kontoeier, som ønsker å gjennomføre en pengeoverføring via nett, kommer ikke unna kontotilbyder, men kan fint klare seg uten et fullmaktforetak.

[8] Directive (EU) 2015/849
[9] Directive 2005/60/EC
[10] PSD2, artikkel 4 (18); Se kapittel 2
[11] PSD2, artikkel 4 (17); Se kapittel 2
[12] Saltkjel (2019)

Kontotilbyder blir slik også den som er nærmest å kunne pulverisere kostnadene med anti-hvitvaskingstiltak. For eksempel kan betaler ilegges valutavekslingsgebyrer og andre transaksjonsgebyrer, og kontotilbyder kan låne ut kundemidler som er under oppbevaring mellom overføringer, og i tillegg drive mersalg til kunden i form av andre finansielle tjenester.

Samtidig er fullmaktforetakene underlagt det samme anti-hvitvaskingsregelverket som kontotilbyderne. Fullmaktforetak må foreta risikovurderinger både av kunder og transaksjoner, gjennomføre kundetiltak og utføre undersøkelser av reelt eierskap. Fullmaktforetakene har også undersøkelsesplikt, og påfølgende rapporteringsplikt for mistenkelige transaksjoner. Et spørsmål som gjør seg gjeldende, er da om anti-hvitvaskingspliktene i AMLD4 for fullmaktforetak når et slikt omfang at de sett i lys av fullmaktforetakenes rolle i transaksjonene, kommer i faktisk motstrid med formålene i PSD2.

Etter innføringen av PSD2 har det hersket usikkerhet om hvordan hvitvaskingsregelverket i AMLD4 anvendes på fullmaktforetakene.[13] I lys av dette oppstår flere spørsmål. For det første, i hvilken grad foreligger det faktisk motstrid mellom regelverket i AMLD4 og PSD2 for fullmaktforetak?

For det andre, får reglene i AMLD4 effekt for transaksjoner over visse minimumsbeløp og kundeforhold. Et neste spørsmål blir da under hvilke omstendigheter fullmaktforetak har kundeforhold?

For det tredje, i de tilfellene hvor fullmaktforetak oppfyller inngangsvilkårene i AMLD4, blir et neste spørsmål i hvilken grad og på hvilken måte utgjør fullmaktforetakene en hvitvaskingsrisiko?

For det fjerde, fullmaktforetakene kan som tidligere påpekt, verken holde, motta eller videreføre kundemidler, men kan koble seg på systemene til kontotilbydere og tre inn i kundens posisjon i transaksjonen. Et spørsmål blir da i hvor stor grad fullmaktforetakenes ansvar strekker seg i spørsmål om hvitvasking?

Og for det femte, bør regelverkene i AMLD4 og PSD2 for fullmaktforetakene forenes?

[13] Grohé (2018)

1.2 Aktualitet

Betaling er en del av den essensielle infrastrukturen i samfunnet og er i rivende utvikling. På få tiår har betaling beveget seg fra å være tilnærmet monopolisert av banknæringen, til å bli en integrert del av ikke-banker, som for eksempel WeChat, en kinesisk mobilapp. Med sine 1,51 milliarder brukere, er appens integrerte betalingsløsning, WeChat Pay, en av verdens største betalingstjenestetilbydere.[14]

Ny finansteknologi som WeChat og andre tjenester, har fremtvunget nytenkning fra europeiske lovgivere for å tilpasse regelverket til samtiden og tilby europeiske finansforetak og europeiske forbrukere et trygt juridisk rammeverk i en global verden.

PSD2 utvidet åpningen i det indre markedet for betalingsinstitusjoner. Konsekvensen er at et betalingsforetak på for eksempel Kypros eller Malta mer eller mindre fritt kan tilby sine betalingstjenester til personer i Norge.

Samtidig er kampen mot hvitvasking stadig på dagsordenen. En metastudie estimerte det globale utbyttet fra kriminalitet i 2009 til 1,6 billioner dollar, tilsvarende 2,7% av verdens samlede bruttonasjonalprodukt.[15] I EU ble det anslått til å omfatte 110 milliarder euro årlig, hvorav 2,2% ble beslaglagt eller frosset, og halvparten, 1,1%, til slutt ble konfiskert i 2010.[16] Hvitvasking kompliserer trolig dette arbeidet betydelig.

Temaet får stadig fornyet aktualitet, også i sammenheng med covid-19 pandemien. Den nye normalen åpner for nye muligheter for kriminelle som ønsker å vaske penger. En rekke samfunnsfunksjoner ble over natten tvunget over til digitale flater. Dette skaper et mulighetsrom for personer som vil hvitvaske, kan utnytte. Behovet for raske avgjørelser, mangel på varer og begrensninger på fysiske møter, er alle faktorer som legger til rette for aktiviteter som egner seg for hvitvasking. Jain peker på både falske veldedighetsorganisasjoner, private lån og omsetning av smittevernsutstyr som eksempler på nye aktiviteter hvitvaskere kan utnytte for å få overskudd fra kriminalitet inn i den legale økonomien.[17]

1.3 Avgrensninger

Videre vil det bli nødvendig å foreta noen avgrensninger. For det første avgrenses oppgaven til betalingsforetak som kun har konsesjon som fullmaktforetak. Det vil si, betalingsforetak som enten har konsesjon som betalingsfullmektig eller opplysningsfullmektig eller begge deler. Avgrensningen

[14] MerchantSavvy.co.uk (2020)
[15] United Nations Office on Drugs and Crime (2011), s. 9
[16] Savona & Riccardi (2015); European Police Office (2016), s. 4
[17] Jain (2020)

er nødvendig for å belyse de særlige utfordringene som gjelder for fullmaktforetak i lys av hvitvaskingsregelverket. Andre finansforetak som også har konsesjon som fullmaktforetak, vil også være rapporteringspliktig på grunnlag av annen konsesjonsbetinget virksomhet.

For det andre avgrenses det til fullmaktforetaks virksomhet i EØS-området. PSD2 har et likt geografisk omfang. Fullmaktforetaket kan likefullt i medhold av konsesjon i foretakets hjemstat og nasjonal rett i kontoeiers hjemstat, yte betalingstjenester tilsvarende eller lik de som er tillatt for foretaket å tilby i hevd av PSD2. Avgrensningen gjøres fordi betalingstjenestevirksomhet begrenset til det indre markedet ofte vil ha en lavere iboende risiko enn betalingstjenestevirksomhet som også involverer personer i tredjeland.

For det tredje avgrenses det til regelverket slik det følger av PSD2 og AMLD4. Norsk lov vil ikke bli kommentert spesifikt. Dette for å få frem de prinsipielle spørsmålene som særlig trer frem i en slik sammenligning.

1.4 Videre fremstilling

For å undersøke hypotesen, vil det først være nødvendig å undersøke fullmaktforetakenes rettslige stilling etter PSD2.[18]

I det neste vil jeg presentere formålshensynene i PSD2 for introduksjonen av fullmaktforetak.[19] Deretter vil det være nødvendig å gå inn i hvilke plikter og krav som følger av AMLD4 for fullmaktforetak.[20] Dette er nødvendig for å undersøke om det er foreligger en motstrid mellom formålene i PSD2 og anti-hvitvaskingspliktene i AMLD4.

Etter dette er det nødvendig å undersøke i hvilken grad fullmaktforetakene representerer en hvitvaskingsrisiko, for slik å kunne gjøre en sammenstilling og undersøke hvilken virkning de totale kravene og pliktene etter AMLD4 har for fullmaktforetakene, og hvordan dette står seg i lys av PSD2.[21]

Avslutningsvis vil det bli fremmet en konklusjon, for så å runde av med noen rettspolitiske betraktninger.[22]

[18] Se kapittel 2.
[19] Se kapittel 3.
[20] Se kapittel 4.
[21] Se kapittel 5.
[22] Se kapittel 6 og 7.

2 Introduksjon til fullmaktforetak

2.1 Innledning

PSD2 ble innført 13. januar 2018 i EU, og erstattet med dette PSD1 fra 2009. Formålet med PSD1 var å fremme konkurranse og deltakelse i det europeiske markedet for betalingstjenester. Gjennom PSD1 ble det etablert et felleseuropeisk regelverk som åpnet opp for at betalingsforetak uten konsesjon til å drive bankvirksomhet, kunne tilby betalingstjenester.

I likhet med PSD1 er PSD2 et fullharmoniseringsdirektiv.[23] At direktivet er fullharmoniserende betyr at nasjonal rett i den enkelte medlemsstat ikke kan avvike fra reglene eller bestemmelsene i direktivet, med mindre direktivet gir spesifikt anledning til dette for den enkelte rettsregelen.

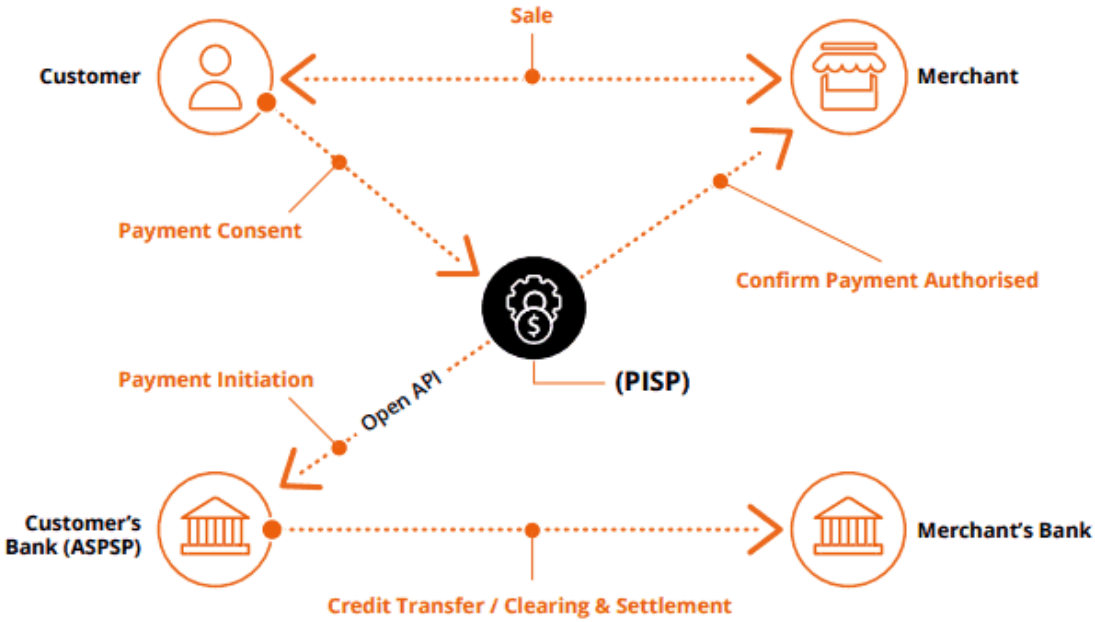
En viktig nyvinning i PSD2 var introduksjonen av reguleringer for fullmakttjenester. I praksis skjedde dette ved å utvide direktivets omfang, og ved å introdusere en ny kategori betalingsforetak, fullmaktforetak, også kalt tredjepartsleverandører.

Spennet av fullmakttjenester er vidt og strekker seg fra andre banker som ønsker å åpne opp for at bankkunder fra konkurrenter skal kunne ta med seg kundedata til dem, til digitale betalingstjenester som for eksempel Vipps, og andre aktører som ønsker å integrere betaling som en del av sitt produkt eller sin tjeneste, for eksempel nettbutikker.[24] Effektivt sett fjernet direktivet med dette bankenes monopol på informasjon om og tilgang til kundenes kontoer.

Fullmaktforetakene kalles tredjepartsleverandører, fordi de ikke nødvendigvis er betalingsforetak eller andre typer finansforetak, og slik sett står utenfor den ordinære betalingskjeden.

Det er to typer fullmaktforetak: betalingsfullmektiger og opplysningsfullmektiger.

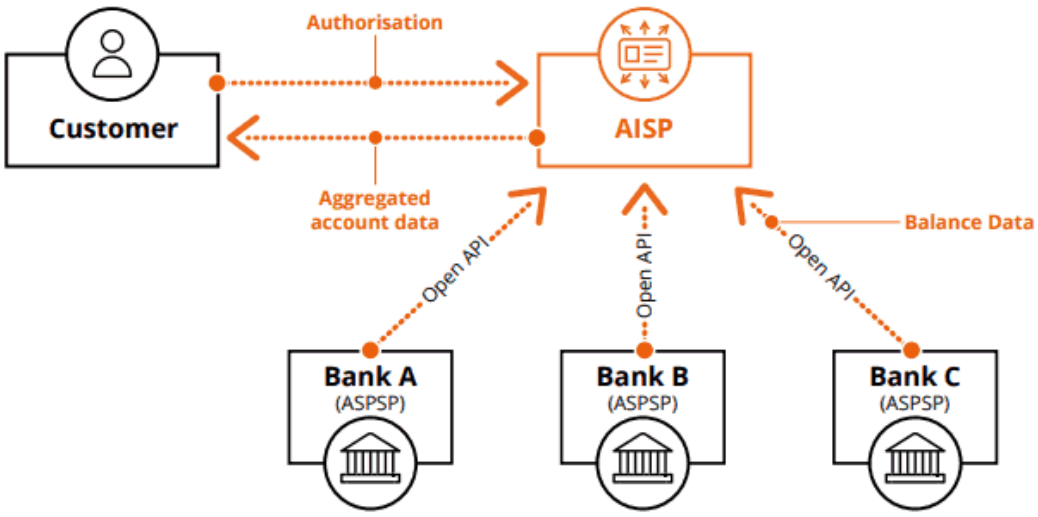
[23] PSD2, artikkel 107 nr. 1; PSD1, artikkel 86, nr. 1
[24] Hernæs (2019); Mathias (2019)



Figur 1: Illustrasjon av betalingsinitieringstjeneste utført av en betalingsfullmektig.[25]

Betalingsfullmektiger har konsesjon til å tilby betalingsinitieringstjenester. Betalingsinitieringstjenester er å "initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider".[26] Betalingsinitiering er altså å initiere en overføring fra en betalingskonto til en betalingsmottaker – eksempelvis en næringsdrivende, som illustrert ovenfor.[27]

[25] Bolton (2020)
[26] PSD2, artikkel 4 (15)
[27] Se figur 1.



Figur 2: Illustrasjon av kontoopplysningstjeneste utført av en opplysningsfullmektig.[28]

Opplysningsfullmektiger har konsesjon til å tilby kontoopplysningstjenester[29]
Kontoopplysningstjenester er en "online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider".[30] Kontoopplysning er altså å fremstille kontohistorikken fra en eller flere betalingskontoer med samme kontoeier.

Kontoeier har etter PSD2 rett til å benytte betalingsinitieringstjenester og kontoopplysningstjenester tilbudt av fullmaktforetak, om kontoeiers "payment account" som er tilgjengelig på nett.[31] Det er fortsatt uavklart hvor den eksakte avgrensningen for "payment account" går.[32] Definisjonen av "payment account" i PSD2 er lik den i PSD1.[33] Slik gir en prejudisiell avgjørelse om definisjonen av "payment account" i PSD1 fra EU-domstolen noe veiledning i spørsmålet om definisjonen av betalingskonto.

Spørsmålet i saken vedgikk hvorvidt en sparekonto var en betalingskonto etter PSD1. Kontoeier kunne fritt overføre fra sparekontoen uten straffegebyrer eller tilbakebetaling av renter, men kunne ikke utføre betalinger direkte fra sparekontoen. Pengene måtte først overføres til en brukskonto. I avgjørelsen stilte domstolen opp krav om at kontoen måtte kunne brukes i "day-to-day payment transactions".[34]

[28] Bolton (2020)
[29] PSD2, artikkel 4, (19), smh. Annex II, punkt 8
[30] PSD2 artikkel 4 (16)
[31] AMLD4, artikkel 66 (1); artikkel 67 (1)
[32] Furset (2021); Beyrouthy (2021)
[33] PSD2, artikkel 4, punkt 12; PSD1, artikkel 4, punkt 14
[34] C-191/17, avsnitt 28

Videre påpeker retten at kontoproduktets navn er i seg selv ikke avgjørende, og at det beror på en konkret vurdering av funksjonaliteten.[35] Som et minimum må kontoeieren kunne "place funds", "withdraw cash", og "execute and receive payment transactions [...] to and from a third party".[36] Minimumskravene til en betalingskonto er altså at man skal kunne foreta innskudd og uttak samt gjennomføre betalinger til tredjemann direkte fra kontoen.

Her foreligger det altså en rettsuklarhet. For oppgavens hovedspørsmål faller dette imidlertid utenfor ettersom kontotype ikke er av relevans for hvorvidt anti-hvitvaskingspliktene i AMLD4 får effekt. Jeg vil derfor ikke gå inn i ytterligere drøftelser av betalingskonto.

Det sentrale er at betalingsfullmektig ikke kan oppbevare kundemidler som en del av leveringen av betalingsinitieringstjenesten.[37] Det samme gjelder for den opplysningsfullmektige. Et fullmaktforetak vil i praksis kun tre inn i kontoeiers sted som et alternativ til å logge direkte inn i nettbanken.

Begge fullmakttjenestene forutsetter kontoeiers samtykke.[38] Dette innhentes ved hjelp av sterk kundeautentisering som forutsetter bruk av minst to av tre metoder for å bekrefte identitet: noe kunden har, er eller vet.[39] Noe kunden har, kan eksempelvis være en BankID-brikke, mens noe kunden er, kan være fingeravtrykk, og noe kunden vet, et passord.

Fullmaktforetaket kan ikke utøve større rett enn den kontoeier selv har. Der hvor en konto har flere enn en eier, vil utøvelsen av fullmakttjenesten bero på den enkelte kontoeiers rettigheter.

I praksis henter fullmakttjenestene informasjonen fra kundenes bankkontoer via en av to metoder. Primært skjer dette gjennom bruk av programvaregrensesnitt (API), alternativt skjer dette ved skjermskraping.[40] Fordi skjemskraping fordrer at tredjeparten har tilgang til kundenes kontoer direkte, og vil kunne avlese informasjon som en bruker, er det en klar preferanse for bruk av API blant bankene.[41] Bruk av API er også kostnadsreduserende for fullmaktforetakene, ettersom majoriteten av europeiske banker omfattet av PSD2, tilbyr API etter ett av tre standardiserte rammeverk.[42]

Det er dermed klart hva et fullmaktforetak er, og hvordan de utøver sin virksomhet. I det neste vil oppgaven redegjøre for formålene i PSD2, og hvordan fullmaktforetakene medvirker til oppfyllelsen av disse.

---

[35] C-191/17, avsnitt 29
[36] C-191/17, avsnitt 30
[37] PSD2, artikkel 66, punkt 3, bokstav a
[38] PSD2, artikkel 97 (1), bokstav a-b
[39] Commission Delegated Regulation (EU) 2018/389, avsnitt 6
[40] Yapily.com (2020)
[41] European Banking Federation (2017)
[42] Johnsen (2019)

3 Formålene i PSD2

3.1 Innledning

Oppgavens hovedspørsmål bygger på hypotesen om at det foreligger motstrid mellom formålene i PSD2 og anti-hvitvaskingspliktene i AMLD4. Det vil derfor være nødvendig med en gjennomgang av nettopp formålene i PSD2.

PSD2 videreførte prosjektet man startet på i PSD1. Det var etter innføringen av PSD1 klart at flere nye innovative betalingsprodukter og tjenester falt utenfor de rettslige rammene av det originale direktivet.[43] Den juridiske usikkerheten gjorde det vanskelig for visse betalingsprodukter og tjenester å lansere trygge og innovative nyvinninger som også var enkle i bruk i det europeiske markedet.[44] Det var behov for å sikre både næringslivet og forbrukere et juridisk rammeverk, derav PSD2.

PSD2 har ingen egen formålsparagraf, men viser til fem hensyn Den europeiske banktilsynsmyndighet skal legge til grunn når en teknisk standard utarbeides. Det første er å sørge for en sikkerhetsmessig minimumsstandard for betalingstjenestebrukere og betalingstjenesteleverandører. Det andre er å beskytte kundemidler og personsensitive opplysninger. Det tredje er å sikre og opprettholde rettferdig konkurranse mellom betalingstjenestetilbyderne. Det fjerde er å sikre teknologi- og forretningsmodellnøytralitet. Og det femte er å tillate utviklingen av brukervennlige, tilgjengelige og innovative betalingsmetoder.[45]

I det videre vil jeg ta utgangspunkt i denne inndelingen av formålene, men slå sammen hensynet til sikkerhet, personvern og kundemidler ettersom dette i praksis er ulike sider av regelverket for IT-sikkerhet.[46] Som et særlig formål vil jeg legge til å sikre forbrukerrettigheter , da dette vies særlig oppmerksomhet i direktivets fortale og Europakommisjonens pressemelding i forbindelse med lanseringen av direktivet.[47]

I det videre vil de enkelte hensynene gjennomgås grundigere med formål om å tilføre et bedre fundament for senere å kunne se pliktene i AMLD4 i lys av de nå påfølgende formålene i PSD2.

[43] PSD2, fortalen, avsnitt 4
[44] PSD2, fortalen, avsnitt 4
[45] PSD2, artikkel 98 (2), bokstav a-e
[46] Se PSD2, fortalen, avsnitt 94-96; også gruppert samlet i
[47] PSD2, fortalen, avsnitt 4; European Commission (2015)

3.2 Sikkerhet, kundemidler og personsensitive opplysninger

Det første formålet med PSD2 er å stille krav til sikkerhet for brukere og tilbydere samt å sikre kundemidler og personsensitive opplysninger. Dette er i stor grad ivaretatt for fullmaktforetakenes del gjennom krav om sterk kundeautentisering, og er det samme kravet som gjelder for pålogging til kontotilbyders egen nettløsning.[48] Har man urettmessig tilgang via et fullmaktforetak, har man i praksis det samme direkte hos kontotilbyder. En person som ønsker å misbruke en annens konto for hvitvasking, vil dermed ikke vinne større rett ved å benytte seg av fullmakttjenester.

Videre vil verken betalingsfullmektig eller opplysningsfullmektig holde kundemidler. For betalingsfullmektige er dette spesifikt uttalt i PSD2, mens for opplysningsfullmektige har trolig lovgiver ikke ansett det som nødvendig, tatt i betraktning kontoopplysningstjenesters naturlige begrensninger.[49]

I fortalen påpekes det at "safe and secure payment services constitute a vital condition for a well-functioning payment services market".[50]

En lovregulering av fullmakttjenestene sørger for at det settes rammer for hvordan, og under hvilke omstendigheter, fullmaktforetak kan behandle personopplysninger.

Fullmaktforetak kan ikke etterspørre mer informasjon fra kontotilbyder, enn det som er nødvendig for å tilby tjenesten.[51] Dette skal imidlertid ikke forstås som et hinder for anti-hvitvaskingstiltak.[52]

For at markedet skal fungere effektivt, og nye tilbydere skal få tillit av brukerne, er det viktig at brukernes sikkerhet ivaretas. Færre ville være villige til å prøve en ny tjeneste fra en ny tilbyder, om man løp en større risiko for å ende opp med tom bankkonto og ingen å holde ansvarlig. Dette er også et poeng som fremheves i grønnboken "Towards an integrated European market for card, internet and mobile payments", som er en analyse av rettsvirkningen av PSD1 for betalingstjenester, og henvises til i fortalen i PSD2.[53]

EU-direktivers forarbeider har mindre rettskildemessig verdi enn norske forarbeider fordi de i mindre grad brukes av EU-domstolen enn hva som er praksis i norsk rett. Forarbeider kan imidlertid brukes som støttemomenter i formålstolkning. Fordi grønnbøker kommer tidlig i lovutviklingsprosessen, har

[48] PSD2, artikkel 97 (1), bokstav a-b
[49] PSD2, artikkel 67 (2), bokstav a
[50] PSD2, fortalen, avsnitt 7
[51] PSD2, artikkel 66 (3), bokstav g; artikkel 67 (2), bokstav f
[52] Guidelines 06/2020, avsnitt 20-25
[53] PSD2, fortalen, avsnitt 4

den også mindre vekt. Grønnbøker er imidlertid fortsatt en del av tilblivelseshistorien til direktivet. Dermed får også grønnbøker relevans i bekreftelse eller avkreftelse av ulike tolkningsalternativer.[54]

3.3 Rettslig vern for forbrukerne

Det andre formålet med PSD2 er å styrke vernet av forbrukerne og sikre deres rettigheter.

Forbrukerrettighetene styrkes av sikrere betalingstjenester, et rettslig vern av kundemidler og personsensitive opplysninger. Fraværet av reguleringer har skapt et lovmessig tomrom, som har vært til skade for forbrukernes rettslige vern, ifølge fortalen:

"Furthermore, the scope of [PSD1] and, in particular, the elements excluded from its scope, such as certain payment-related activities, has proved in some cases to be too ambiguous, too general or simply outdated, taking into account market developments. This has resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas".[55] Ambisjonen om å styrke forbrukernes rettigheter med PSD2, er slik et uttrykk for at man i tiden etter PSD1 har sett, på et EU-rettslig plan, et lovmessig tomrom, som følge av at nye produkter og tjenester er blitt introdusert.

Tomrommet, slik det beskrives i fortalen, har ført til manglende rettslig vern.[56] Fullmakttjenester er et eksempel på tidligere uregulerte betalingstjenester, som med PSD2 reguleres, og slik sikrer et felles vern av forbrukerrettighetene i EØS-området.

Forbrukerne er også tjent med et harmonisk og klart regelverk. I de tilfellene hvor kontoeier er en forbruker, vil forbrukeren være den svakere parten i relasjonen mellom kontoeier og kontotilbyder. Den svakeste parten vil ha klare fordeler av et forutberegnelig regelverk som gir grunnlag for å løse konflikter utenfor rettssystemet.

Forbrukernes stilling styrkes gjennom bedre konkurranse og innovasjonskraft, som begge vil lede til bedre produkter og tjenester, og lavere priser.

3.4 Brukervennlige, tilgjengelige, og innovative tjenester

Det tredje formålet med PSD2 var å sikre rammevilkårene for utvikling av brukervennlige, tilgjengelige og innovative tjenester.

[54] Strømsnes (2021)
[55] PSD2, fortalen, avsnitt 4
[56] PSD2, fortalen, avsnitt 4

I Europakommisjonens pressemelding i forbindelse med PSD2, trekkes særlig betalings- og opplysningsfullmektiger frem.[57]

Med et harmonisert regelverk, kan eksisterende og nye aktører enklere og med en lavere kostnad, utvide tjenestetilbudet sitt til flere medlemsstater enn hjemstaten. Slik stimuleres det også til innovasjon. Et større felles marked gir rom for kostnadsbesparelser og øker inntektspotensialet. Et felles indre marked med et harmonisert regelverk, gir tilbydere en lavere barriere for å entre markeder i andre medlemsstater enn hjemstaten.

I grønnboken fremheves det også at "Europe has an opportunity to be at the cutting edge of what 'making a payment' could mean in the future". Lovgiver ser altså for seg Europa som et potensielt arnested for ny finansteknologi for betalingstjenester. Et integrert og effektivt marked vil bedre forutsetningene for at den europeiske finansteknologinæringen skal lykkes med dette. Det fremheves spesifikt at man nå ikke lenger er låst til "two existing international card schemes".[58]

For fullmaktforetak vil det for eksempel kunne gjelde spørsmål om finansiell inkludering. PSD2 sikrer alle kontoeiere tilgang til sine kontoer via fullmaktforetak. Dette representerer et skifte fra tiden før PSD2, hvor API-tilgang og mulighetene det gir for å benytte produkter og tjenester, var begrenset, både i form av at det ikke var tilgjengelig hos alle kontotilbydere, og tilbudet oftest ikke var allment tilgjengelig.

3.5 Rettferdig konkurranse mellom alle tilbydere

Det fjerde formålet med PSD2 er å sikre en fortsatt rettferdig konkurranse mellom alle tilbydere. Rettferdig konkurranse forutsetter integrasjon på tvers av statene. Særlig er dette av betydning for fullmaktforetak som er heldigitale virksomheter, og fritt kan tilby tjenester i alle statene i det indre markedet i hevd av konsesjon i en stat.

Ved at konkurransen øker, vil også kostnader og gebyrer på betalingstjenester presses ned og, ikke minst, utfordre de eksisterende tilbyderne av betalingstjenester.[59]

[57] European Commission (2015)
[58] COM/2011/0941, s. 2-3
[59] COM/2011/0941, s. 2

3.6 Teknologi- og forretningsmodellnøytralitet

Det femte formålet med PSD2 er å sikre et teknologi- og forretningsmodellnøytralt regelverk.

Dette er også tydelig presisert i direktivets fortale: "This Directive should aim to ensure continuity in the market, enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework".[60]

For å lykkes med ambisjonen om å utvikle fremtidens betalingsmetoder, er det også fundamentalt at det begynnende duopolet som skisseres i grønnboken, utfordres i tilstrekkelig grad, også av nye aktører.[61] Nettopp behovet for "common open standards" fremheves også i grønnboken.[62]

Å sikre tilgang til nye tilbydere, er også et formål som påpekes i direktivets fortale; "this Directive should aim to ensure continuity in the market, enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework".[63] Denne forståelsen støttes også av at regelverket skal være "clear". Et klart regelverk vil være anvendbart på aktører på tvers av vertikaler og markeder.

3.7 Oppsummering av formålene i PSD2

I det forutgående har formålene i PSD2 blitt gjennomgått. Vi har sett at det på tvers av de nasjonale markedene i EØS-området, finnes en rekke ulike betalingsmetoder, og at to kortnettverk står for et begynnende duopol.

Introduksjonen av fullmaktforetakene som nye aktører, senker terskelen for handel på tvers av nasjonalgrensene. Indirekte vil det også få en positiv effekt på fri flyt av arbeidskraft ved at EØS-borgere hjemmehørende i en stat, kan flytte til en annen EØS-stat, og beholde sine eksisterende kontoforhold, og likevel fritt bruke betalingstjenester tilbudt av fullmaktforetak i vertsstaten.

PSD2 er en forutsetning for å sikre tilgangen til markedet for fullmaktforetakene. Uten et lovpålegg om at alle kontotilbydere i EØS-området må gi fullmaktforetakene API-tilgang, ville det neppe vært realistisk å få et velfungerende system på EU-nivå som inkluderer en majoritet av kontotilbyderne i Europa.

[60] PSD2, fortalen, avsnitt 33
[61] COM/2011/0941, s. 2-3
[62] COM/2011/0941, s. 6
[63] PSD2, fortalen, avsnitt 33

Betalingstjenester lik eller lignende fullmakttjenester ble allerede før PSD2 tilbudt av enkelte aktører i enkelte stater, og da regulert som en "Technical Service Provider" etter PSD1.[64] Ved å lovregulere fullmaktforetak spesifikt, sikrer man minimumsstandarder med hensyn til sikkerhet og forbrukerrettigheter, til det beste for både tilbydere og brukere.

PSD2 utfordrer ikke bare det internasjonale banksystemet teknologisk, men representerer også en revolusjon i forholdet mellom aktørene innenfor betaling. Man går fra å ha et system med høye inngangsterskler, og historisk sett svært høy tillit aktørene imellom, til et system som i større og større grad ansvarliggjør hver enkelt aktør for å håndheve regelverk for forbrukervern, sikkerhet, personvern og anti-hvitvasking. Ved å introdusere fullmakttjenester, oppstår en rekke potensielle konflikter mellom ønskene om et åpent og transparent fritt marked og regelverket for anti-hvitvaskingsarbeid. I det neste gjennomgås derfor anti-hvitvaskingspliktene for fullmaktforetakene, slik de følger av AMLD4.

4 Pliktene i AMLD4

4.1 Innledning

AMLD4 har som formål å forhindre at det europeiske finanssystemet blir misbrukt "for the purposes of money laundering and terrorist financing".[65] AMLD4 er det fjerde av en serie direktiver som tar sikte på å skape en felles EU-rettslig plattform for anti-hvitvaskingsarbeidet i det indre markedet.

AMLD4 bygger på anbefalingene fra Financial Action Task Force (FATF).[66] AMLD4 har imidlertid ikke som mål å fullharmonisere regelverket slik PSD2 har, men utgjør krav til en minimumsstandard for medlemsstatenes anti-hvitvaskingsregelverk. Medlemsstatene står fritt til å innføre strengere regler enn de reglene AMLD4 legger opp til, innenfor grensene av unionsretten.[67]

Av AMLD4 følger et sett med verktøy oppnå dette.[68] Verktøyene er det som kan kalles de rapporteringspliktiges plikter. Alle rapporteringspliktige, inklusive fullmaktforetak, er pålagt å håndheve dette regelverket.

[64] PSD1, artikkel 3, bokstav j
[65] AMLD4, artikkel 1, punkt 1
[66] Rui (2012), s. 85 og 236
[67] AMLD4, artikkel 5
[68] AMLD4, artikkel 45

Anti-hvitvaskingspliktene kan grupperes på ulike måter. For oppgavens del har jeg valgt å dele dem inn i fire grupper: risikovurderinger, kundetiltak, opplysninger om reelt eierskap og rapporteringsplikt.

Øvrige anti-hvitvaskingsplikter kan for fullmaktforetakenes del anses som følgekonsekvenser av disse fire anti-hvitvaskingspliktene. For eksempel vil plikten til å identifisere og vurdere risikofaktorer begge være naturlige konsekvenser av at fullmaktforetakene er pålagt å utføre risikovurderinger. Denne firedeling av regelverket gjør også anti-hvitvaskingspliktene egnet for senere drøftelser i lys av PSD2.

Oppgavens hovedspørsmål er om den totale summen av disse pliktene når et slikt omfang at AMLD4 kommer i strid med de forutgående drøftede formålene i PSD2.

I det videre vil hver av de respektive pliktene i AMLD4 omtales nærmere for å se hvordan de slår ut for fullmaktforetakene, for slik å senere kunne se de i lys av formålene i PSD2.

4.2 Risikovurderinger

Den første av anti-hvitvaskingspliktene i AMLD4, er risikovurdering.

Risikovurderingene har to steg: identifisering og vurdering. AMLD4 stiller krav om at minimum tre grupper risikofaktorer skal vurderes: risikoen som følger av forhold ved kunden, den geografiske risikoen og landrisikoen, samt produkt-, tjeneste-, transaksjons-, og distribusjonskanalrisiko.[69]

Den første gruppen risikofaktorer er kunderisikofaktorer. Det er de risikofaktorene som følger av forhold ved kundens person, virksomhet eller øvrige omstendigheter ved forretningsforholdet.

Som minimum skal fullmaktforetak risikovurdere tilfeller hvor kunden gjør flere overføringer til samme betalingsmottaker.[70] Ettersom beløpsgrensene er godt kjent, vil det også være sannsynlig at hvitvaskere forsøker å unngå undersøkelser fra rapporteringspliktige ved å splitte opp transaksjoner. Fullmaktforetaket skal i disse tilfellene vurdere det økonomiske eller legitime rasjonale, og om betalingen er splittet for å unngå beløpsgrenser for enkelttransaksjoner.[71]

Den andre gruppen risikofaktorer er geografiske. Disse inkluderer risikofaktorene som følger av både virksomhetens og kundenes geografiske plassering.

[69] AMLD4, artikkel 8 (1)
[70] EBA/GL/2021/02, s. 85
[71] Se 4.2.3.1 om kombinerte transaksjoner & 4.5.1.1 om beløpsgrenser

Fullmaktforetak er digitale selskaper som i hevd av konsesjon i en EØS-stat, kan tilby sine fullmakttjenester i hele EØS-området. Tilbyr fullmaktforetaket tjenester utenfor hjemstaten, vil dette med andre ord være en risikofaktor som er særlig aktuell. Fullmaktforetak skal vurdere den risikoen som følger av at de har kunder hjemmehørende i en annen stat enn selskapets egen hjemstat, for eksempel ved å sjekke ulike landrisikovurderinger.[72]

Såfremt det dreier seg om kunder hjemmehørende i andre EØS-stater, vil det være en begrenset risiko.[73] Nasjonale tilsynsmyndigheter er likevel oppfordret til å håndheve regler som sikrer rutiner hos de rapporteringspliktige for å avklare hvorfor kunder fra andre stater ønsker å benytte betalingstjenesten.[74]

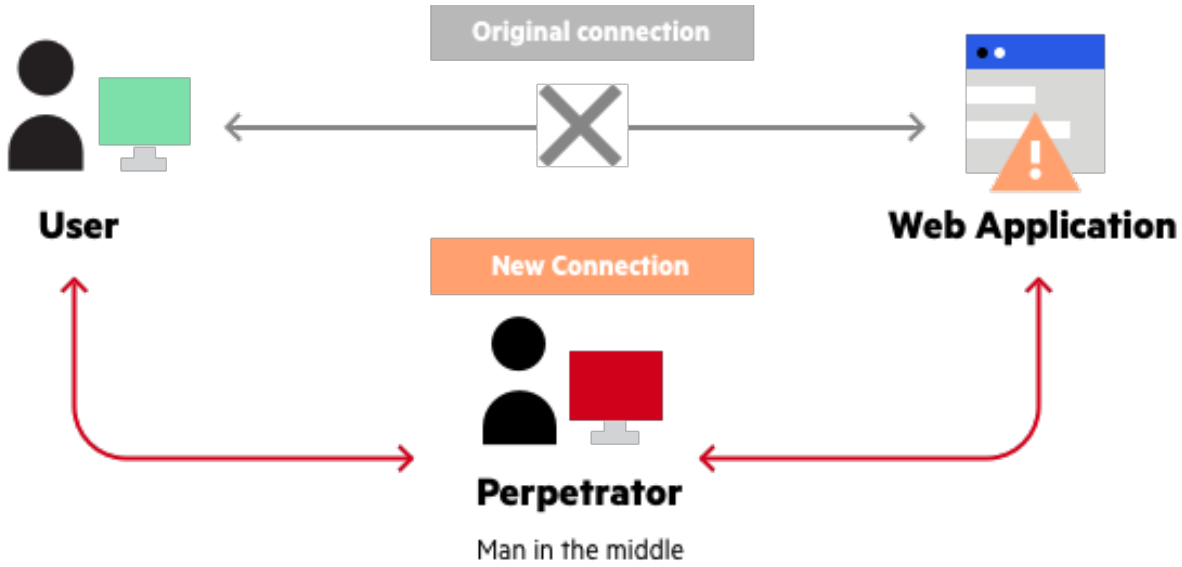
Den tredje gruppen risikofaktorer er produkt-, tjeneste-, transaksjon- og distribusjonskanalrisiko.[75] Det er risikoen som følger av fullmaktforetakenes egne produkter og tjenester. I det videre vil jeg presentere tre eksempler på dette som er relevant for fullmaktforetak.

4.2.1 Kombinerte transaksjoner

Betalingsfullmektiger vil kunne tilby en kontoeier å gjennomføre en betaling ved å trekke fra kundemidler fra flere kontoer hos flere kontotilbydere. Etter AMLD4 vil en slik transaksjon være likestilt med en transaksjon på det samlede beløpet fra en enkelt konto.[76] En hvitvasker vil da kunne gjennomføre det som for egne kontotilbydere, og betalingsmottakers kontotilbyder, fremstår som en serie overføringer av lavere verdi, men som samlet sett utgjør en felles transaksjon av høyere verdi.

[72] AMLD4, Annex III; Annex III; se for eksempel Basel AML index
[73] AMLD4, Annex II
[74] JC 2017 81, s. 17
[75] EBA/GL/2021/02, s. 26
[76] AMLD4, artikkel 11, bokstav b (i)

4.2.2 Mannen-i-midten-angrep



Figur 3: Et eksempel på et mannen-i-midten-angrep.[77]

Mannen-i-midten-angrep er et kryptografisk begrep for å beskrive det tilfellet hvor en angriper for eksempel utgir seg for å være den ene parten i et topartsforhold hvor partene tror de kommuniserer direkte, for å utnytte begge eller den andre.[78] En betaler vil kunne utsettes for et mannen-i-midten-angrep ved bruk av betalingsinitieringstjenester, enten ved at den betalingsfullmektige medvirker eller utnyttes uten medviten ved for eksempel datainnbrudd.

Et slikt angrep kan utnyttes til hvitvasking ved at betaler lures til å betale en annen person enn betalingsmottaker, og betalingsmottaker får betalt av en annen person enn betaler. Tilfellet er særlig aktuelt når en hvitvasker ønsker å tilsløre pengenes opprinnelse. En betalingsfullmektig med et høyt antall transaksjoner, vil kunne erstatte behovet for tradisjonelle muldyr. Fordelen for en hvitvasker vil da være lavere kostnader, mindre administrasjon og redusert svinn.

4.2.3 Automatisert hvitvasking

Hvitvasking deles tradisjonelt inn i tre steg: plassering, tilsløring og integrasjon.[79] Ved plassering er man avhengig av å få pengene inn i det finansielle systemet, der fysiske penger må bli til digitale penger. Formålet i tilsløringsprosessen er å tilføre pengene troverdighet. Deretter integreres pengene inn igjen i økonomien, og gis et nytt, falskt opphav.

[77] Imperva.com (u.å.)
[78] Ornaghi & Valleri (2003)
[79] Federal Financial Institutions Examination Council (u.å.)

En uttalt bekymring med introduksjonen av betalingsfullmektiger har vært frykten for automatisert hvitvasking.[80] En hvitvasker kan ved hjelp av kontotilbyders API'er enklere enn tidligere, gjennomføre et ubegrenset antall transaksjoner via et høyt antall kontotilbydere. Å logge inn og legge inn transaksjoner, er betydelig mer tidkrevende, enn å programmatisk initiere betalingstransaksjoner, enten etter et manuelt utarbeidet oppsett, eller generert av dataprogrammet innenfor rammene av forhåndsdefinerte regler.

Automatisering er ikke bare kostnads- og risikoreduserende, men også muliggjørende i seg selv. Som en straffedømt hacker intervjuet i podcasten Darknet Diaries poengterte; det vanskeligste var verken å stjele kortdata, eller å overføre pengene, men å ha kompetente stråmenn som man kan stole på i enden av transaksjonen.[81] Med konsesjon som fullmaktforetak, er det mulig å automatisere hele eller deler av denne prosessen.

I praksis kan en hvitvasker ved hjelp av kontotilbyders API-er gjennomføre et ubegrenset antall transaksjoner via et høyt antall kontotilbydere. Å logge inn og legge inn transaksjoner er betydelig mer tidkrevende enn å programmatisk initiere betalingstransaksjoner, enten etter et manuelt utarbeidet oppsett, eller generert av et dataprogram innenfor rammene av forhåndsdefinerte regler.

Også kontoopplysningstjenester får slik en funksjon for en hvitvasker, både som et kontrollverktøy, for eksempel utarbeidelse av dashbord, og som et administrasjonsverktøy. En kontoopplysningstjeneste kan både varsle om uregelmessigheter som kan gi en hvitvasker indikasjoner om at det utføres undersøkelser, og forenkle administrasjonsarbeidet av stråmenn. Slik medvirkning er også omfattet av AMLD4.[82]

4.3 Kundetiltak

Den andre av pliktene i AMLD4 er kundetiltak. Kundetiltakene skal hjelpe den rapporteringspliktige til å få en bedre risikoforståelse av kundeforhold og transaksjoner.[83]

Kundetiltak er registrering og kontroll av opplysninger om kunder. Det vil alltid være behov for at kunden legitimerer seg for bruk av fullmakttjenester.[84]

Det er tre nivåer av kundetiltak: forenklede, ordinære og forsterkede kundetiltak.

[80] Lammerts et. al. (2017), s. 17, avsnitt 3.3.2
[81] Rhysider (2021)
[82] AMLD4, artikkel 1 (3), bokstav d
[83] EBA/GL/2021/02, s. 38
[84] EBA/GL/2021/02, s. 128

I de tilfellene hvor fullmaktforetakets kunde er kontoeier, vil kontoeier kunne legitimere seg i hevd av kundeforholdet til banken.[85] I de tilfellene hvor fullmaktforetakets kunde er en annen, for eksempel betalingsmottaker for en betalingsfullmektig, vil det ofte være behov for mer enn forenklede kundetiltak.

Avhengig av risikovurderingen av virksomheten, tjenestene og produktene, samt av kunden, foretar man enten forenklede, ordinære eller forsterkede kundetiltak.[86]

I de fleste tilfeller hvor kunden er en naturlig person, vil forenklede kundetiltak være mest relevant for fullmaktforetak, men ved høyrisikosituasjoner, vil forsterkede kundetiltak være nødvendig.[87]

Et eksempel på et slikt tilfelle for et fullmaktforetak, vil være der hvor kunden er en politisk eksponert person (PEP). En PEP er en naturlig person som har eller har hatt et av de offentlige tillitsvervene listet i AMLD4.[88] Er kunden en PEP, skal det gjennomføres forsterkede kundetiltak.[89]

Reglene for PEP gjelder også der hvor kunden er en juridisk person og reell eier er en PEP.

Er kunden en juridisk person, er det ofte nødvendig med registrering og kontroll av opplysninger om reell eier.

4.4 Reelt eierskap

Og det leder til den tredje plikten i AMLD4: bekreftelse av reelt eierskap. Reell eier er definert i AMLD4 som den eller de naturlige personene som i siste rekke eier eller kontrollerer en eller flere juridiske personer som gjennomfører en gitt transaksjon.[90]

Avklaring av reelt eierskap får betydning for fullmaktforetakene i to tilfeller. Det ene er der hvor fullmaktforetaket har en juridisk person som kunde. I dette tilfellet må fullmaktforetaket avklare eierforholdene med hensyn til reglene om reelt eierskap. Det andre er der hvor fullmaktforetaket har en naturlig person som kunde, som er reell eier av en juridisk person, hvor også en politisk eksponert person (PEP) er kunde. Naturlige personer som er reell eier av en juridisk person hvor også en PEP er

[85] EBA/GL/2021/02, s. 129
[86] AMLD4, artikkel 11
[87] EBA/GL/2021/02, s. 128
[88] AMLD4, artikkel 3 (9)
[89] AMLD4, artikkel 20; EBA/GL/2021/02 s. 135
[90] AMLD4, artikkel 3 (6)

reell eier, faller inn under bestemmelsene om "close associates", og får slik konsekvenser for risikovurdering og kundetiltak.[91]

Reelt eierskap av et selskap avhenger av en total vurdering, men direktivet anfører en veiledende grense på mer enn 25% som grense for når en eller flere fysiske personer vil kunne anses som reell eier. Dette skal være uavhengig av om den eller de fysiske personene eier direkte, eller via et eller flere andre selskaper som de selv kontrollerer.[92] Det er altså slik mulig å ha inntil tre ulike naturlige personer som reell eier av samme juridiske person.

4.5 Rapporteringsplikt

Den fjerde plikten i AMLD4, er rapporteringsplikten. Det følger av AMLD4 at alle mistenkelige transaksjoner skal rapporteres, inkludert forsøk på mistenkelige transaksjoner. Terskelen er satt til "reasonable grounds to suspect", altså grunn til å mistenke hvitvasking.[93] Vilkåret om "reasonable grounds" er et minimumskrav, og for eksempel har Norge lagt seg på en strammere linje med vilkåret "forhold som gir grunnlag for mistanke".[94]

Rapportene (MT-meldinger) skal sendes til enhet for finansiell etterretning (FIU) i fullmaktforetakets hjemstat. I det tilfellet hvor et fullmaktforetak sender MT-melding til FIU i egen hjemstat, om en mistenkelig transaksjon fra en kunde hjemmehørende i en annen stat, vil det falle på FIU i fullmaktforetakets hjemstat å videresende meldingen.[95]

Før rapporteringspliktig sender rapport, er det ofte naturlig å gjøre visse undersøkelser. Dette har sågar fått sin form i en egen undersøkelsesplikt.

Undersøkelsesplikten er ikke eksplisitt uttalt i AMLD4, men var opprinnelig det i AMLD1.[96] I AMLD4 er undersøkelsesplikten tatt inn i bestemmelsen om forsterkede kundetiltak.[97] Plikten til å undersøke etter AMLD4 gjelder avklaring av "background" og "purpose" for alle "complex", "unusually large" eller "unusual patterns of" transaksjoner, samt transaksjoner uten "apparent economic or lawful purpose".

[91] AMLD4, artikkel 23
[92] AMLD4, bokstav a, punkt 1
[93] AMLD4, artikkel 33, bokstav a
[94] Hvitvaskingsloven, paragraf 26 (1)
[95] AMLD4, artikkel 53, punkt 1
[96] AMLD1, artikkel 5
[97] AMLD4, artikkel 18 nr. 2

4.6 Oppsummering av pliktene i AMLD4

Rapporteringsplikten og den implisitte undersøkelsesplikten blir slik navet i anti-hvitvaskingsarbeidet, og de forutgående pliktene støtter opp under denne. Risikovurdering av virksomheten og kundeforhold gir grunnlag for anti-hvitvaskingsrutinene som skal avdekke mistenkelige forhold, som i sin tur leder til undersøkelser, og mulig rapportering. Kundetiltak og bekreftelse av reelt eierskap er verktøy for å avklare særlige forhold ved kunden.

Den samlede faktiske virkningen for fullmaktforetak tar form på tre måter. For det første representerer anti-hvitvaskingsplikten en betydelig økonomisk virkning. Bransjeorganisasjonen Financial Data and Technology Association Europe (FDATA) anslo i sin høringsuttalelse til Den europeiske banktilsynsmyndighet, at den samlede kostnaden til anti-hvitvaskingsarbeid for et fullmaktforetak i sitt første driftsår til 772500 euro.[98] Dette er til sammenligning nær 16 ganger egenkapitalkravet for betalingsfullmektiger i Norge.[99]

For det andre representerer anti-hvitvaskingspliktene den sosiale kostnaden som følger av de-risking: betalingstjenestetilbydernes avvisning av kundeforhold som har en uhåndterbar risiko. Avvisning skal bero på en konkret vurdering av kundeforholdet. Det europeiske banktilsynet poengterer også at "de-risking" kan skje ved produkt- og tjenestebegrensninger.[100] Dette rammer både svake grupper som asylsøkere og næringsdrivende i nye næringer som for eksempel kryptovaluta.[101]

For det tredje beløper det også en betydelig mulighetskostnad, slik også FDATA påpeker.[102] Skal betalingsinitieringstjenester kunne utfordre kortbetaling som en reell konkurrent, må de kunne konkurrere på like vilkår. De betydelige merkostnadene anti-hvitvaskingspliktene representerer, vil dermed trolig fordre en proporsjonal gevinst. Flere, inkludert Rui og Søreide, har stilt spørsmål ved om anti-hvitvaskingsarbeidet generelt koster mer enn det smaker.[103] Som en følge av fullmaktforetakenes natur vil det trolig være nødvendig å stille opp et strengere proporsjonalitetskrav enn for kontotilbydende betalingsforetak.

I det videre vil anti-hvitvaskingspliktene for fullmaktforetak drøftes opp mot formålene i PSD2 for å vurdere i hvilken grad de eventuelt alene eller samlet utgjør en faktisk motstrid, for slik å kunne besvare oppgavens hovedspørsmål.

[98] Financial Data and Technology Association Europe (u.å)
[99] Finansforetaksloven 3-4 (2), bokstav b
[100] EBA-OP-2016-07, s. 9
[101] EBA-OP-2016-07 s. 1-3; Hopland (2019)
[102] Financial Data and Technology Association Europe (u.å.)
[103] Rui & Søreide (2020)

5 Forholdet mellom PSD2 og AMLD4

I det forutgående har formålene i PSD2 og pliktene i AMLD4 blitt presentert. I det videre vil jeg se nærmere på forholdet mellom disse to, og hvilken faktisk virkning anti-hvitvaskingspliktene får for fullmaktforetakene i lys av formålene i PSD2.

5.1 Innledning

AMLD4 representerer en minimumsstandard, og åpner slik for variasjoner mellom nasjonale bestemmelser mellom ulike EØS-stater. Samtidig følger direktivet hjemstatsprinsippet, slik at for et fullmaktforetak, vil foretaket kun måtte forholde seg til de nasjonale bestemmelsene i foretakets hjemstat, også i de tilfellene hvor foretaket tilbyr betalingstjenester til personer som hører hjemme i andre EØS-stater.

Oppgavens hovedproblemstilling bygger på hypotesen om at det er en faktisk motstrid mellom disse. For å teste denne hypotesen, er det nødvendig å se regelsettene i sammenheng. I dette kapittelet vil de tidligere presenterte pliktene drøftes enkeltvis i forhold til de tidligere presenterte formålene i PSD2. Av hensyn til struktur presenteres pliktene i samme rekkefølge som i det forutgående kapittelet om pliktene i AMLD4. Først er det imidlertid nødvendig å avklare hvem som er fullmaktforetakets kunde.

Kundeforholdet er hjørnesteinen for AMLD4. Om det foreligger et kundeforhold eller ikke, får konsekvenser for hvordan, overfor hvem, og i hvilken grad, pliktene i AMLD4 skal utøves. For å drøfte pliktene i AMLD4 opp mot formålene i PSD2, er det derfor nødvendig å avklare hvem som er fullmaktforetakenes kunder.

5.2 Hvem er kunden?

Kundeforholdene til det enkelte fullmaktforetaket vil bero på en konkret vurdering av tjenestene og produktene som tilbys, og virksomheten som utøves.[104] Som regel vil det være flere betalere eller betalingsmottakere, og dermed vil det som hovedregel være klart mer arbeidskrevende for fullmaktforetakene om kundeforholdet etableres med betaler, enn med betalingsmottaker.

Foreligger det et "business relationship", skal det nemlig alltid utføres kundetiltak. Foreligger det ikke et slikt kundeforhold, vil hvitvaskingsregelverket først slå ut om transaksjonsgrensene møtes eller overstiges.[105]

[104] EBA/GL/2021/02, s. 10
[105] AMLD4, artikkel 11, bokstav b

“Business relationship” er definert i AMLD4 som et "business, professional or commercial relationship which is connected with the professional activities of an obliged entity", og som "is expected, at the time when the contact is established, to have an element of duration".[106] Det er slik to kumulative vilkår for at et kundeforhold etter AMLD4 er etablert: forholdets art og lengde. Forholdet skal være av forretningsmessig, profesjonell eller kommersiell art, og ha et element av varighet ved seg.

For PSD2 stiller dette seg betydelig annerledes. Et sentralt formål i PSD2 er å utbedre og sikre vilkårene for forbrukere og andre sluttbrukere av betalingstjenester. PSD2 opererer derfor ikke med et tilsvarende kundebegrep som AMLD4, men bruker begrepet “payment service users” om sluttbrukerne, altså betalingstjenestebrukeren, eller mer presist: kontoeier.

Det vil trolig gi et misvisende utfall å tolke direktivene slik at samtlige “payment service users” alltid vil ha et “business relationship” med fullmaktforetaket.

For at det skal foreligge et “business relationship”, må relasjonen partene imellom ha en “business, professional or commercial” art.[107] Det hører trolig til sjeldenhetene at en betalingstjeneste ikke har en forretningsmessig, profesjonell eller kommersiell art.

Relasjonen må også ha være forventet å ha “an element of duration”, altså en viss varighet.[108] Naturlig språklig forståelse tilsier at en enkelt transaksjon ikke er tilstrekkelig for å oppfylle dette kravet.

5.2.1 Betalingsfullmektiger

En viktig motivasjon for introduksjonen av betalingsfullmektiger, var ønsket om et større utvalg av betalingstjenester tilgjengelig for netthandel. I dag er vertikalen som tidligere vist, og påpekt i grønnboken, dominert av to store, internasjonale kortnettverk.[109] Etter AMLD4, har kun banken som utsteder kort kundeforhold til betaler. Et lignende system skisserer Den europeiske banktilsynsmyndighet i retningslinjene til AMLD4 .[110]

Et spørsmål blir da om hvor grensen går for betalingsfullmektiger som eksklusivt tilbyr betalingstjenester til nettbutikker, før de også har et kundeforhold til betaleren.

[106] AMLD4, artikkel 3 (13)
[107] AMLD4, artikkel 3 (13)
[108] AMLD4, artikkel 3 (13)
[109] COM/2011/0941
[110] EBA/GL/2021/02, s. 10; s. 127

Ordinære handelstransaksjoner vil trolig være tilstrekkelig for å oppfylle vilkåret om at forholdet må ha en "business, professional or commercial" art. Det er grunn til å anta at det er få netthandelskjøp som ikke har en forretningsmessig, profesjonell eller kommersiell natur. Ettersom fullmakttjenester er konsesjonsbelagt og regulert, er det vanskelig å se praktiske tilfeller hvor fullmaktforetaket er part i en profesjonell relasjon, og eventuelle unntak vil trolig være teoretisk.

Spørsmålet blir da hvilken terskel som skal legges til grunn i forståelsen av "an element of duration"? Ettersom det typiske tilfellet er en nettbutikk som har et kundeforhold til en betalingsfullmektig som et alternativ til å akseptere kortbetaling, er det trolig en relasjon av noe varighet.

Et vanlig virkemiddel for å skaffe nye kunder og øke eksisterende kunders aktivitet for kortselskapene, er å tilby bonuser og rabatter.[111] Skal en betalingsfullmektig tilby tilsvarende, vil det være betinget av at betaler har gitt samtykke til lagring av personopplysninger. Praktisk sett vil dette ofte løses ved å opprette en brukerkonto. Dersom betaler oppretter en brukerkonto hos den betalingsfullmektige, vil det være rimelig å anta at det også stiftes et kundeforhold mellom den betalingsfullmektige og betaler.

Opprettelsen av en brukerkonto når sin nedre avgrensning mot lagring av betalingsinformasjon lokalt på brukerens enhet ved bruk av informasjonskapsler. Informasjonskapsler tillater brukerens enhet å lagre informasjon fra nettleseren. Betalingsfullmektiger som implementerer en slik skjemahuskfunksjonalitet i sin betalingsinitieringsløsning, etablerer ikke på dette grunnlaget et kundeforhold mellom betalingsfullmektig og betaler.

5.2.2 Opplysningsfullmektiger

Opplysningsfullmektigers kunder er ifølge retningslinjene fra den Den europeiske banktilsynsmyndighet "the natural or legal person who has the contract with [opplysningsfullmektig]".[112] Altså at kunden er personen som har kontrakt med opplysningsfullmektig. Dette er imidlertid å betrakte som en forenkling av reglene. Kundeforholdet vil fortsatt bero på en konkret vurdering av hvorvidt det er etablert et "business relationship" eller ikke. Denne konkrete vurderingen vil igjen bero på forholdets art, og forholdets lengde.

En kontoopplysningstjeneste er en betalingstjeneste, og som innledningsvis påpekt, er det trolig sjelden at en betalingstjeneste ikke har en forretningsmessig, profesjonell eller kommersiell art. Det avgjørende blir da om det etableres et forhold som er forventet å vare en tid.

[111] Pedersen (2021)
[112] EBA/GL/2021/02, s. 128

PSD2 omfatter kun kontoer som allerede er tilgjengelig via nett, og forutsetter gyldig tilgang til kontoen. Derfor er trolig den kommersielle verdien av kontoopplysningstjenester alene noe begrenset. Mange opplysningsfullmektiger vil derfor ha et ønske om å kombinere eller implementere kontoopplysningstjenester med andre tjenester eller produkter.

Jeg vil i det videre anvende regelen på praktiske eksempler, men først minne om at oppgaven er avgrenset til fullmaktforetak som kun er det. De videre drøftelsene vil derfor begrenses til eksempler hvor kontoopplysningstjenester er kombinert med ikke-konsesjonspliktige produkter og tjenester.

Et slikt eksempel er Xero som siden 2011 har tilbudt opplysningstjenester til enkelte av sine kunder. Før PSD2, var dette basert på et avtaleforhold mellom Xero og kontotilbyder. Ved bruk av opplysningstjenestene kunne kunder i enkelte banker eksportere kontoutskriftene direkte til regnskapsprogrammet, for hurtigere og mer effektiv regnskapsføring.[113]

Det er trolig at kunder av regnskapsprogrammer ofte vil ha forhold til leverandøren av en viss varighet. Det er også trolig sjelden tilfeller hvor levering at en tilbyder av et regnskapstjenester ikke tilbyr en tjeneste av forretningsmessig, kommersiell eller profesjonell art. Tilbydere av regnskapsprogram som også er opplysningsfullmektig for å kunne integrere import av kontoutskrifter, vil således trolig som en hovedregel etablere kundeforhold til sine brukere.

Et unntak fra denne hovedregelen kan tenkes for en regnskapstjeneste rettet mot personer som ikke er bokføringspliktig, og kun har behov for tjenesten i kortere perioder. For eksempel i det tilfellet hvor en ad hoc-komité som organiserer hjelp til ofre etter et leirskred, har behov for regnskapstjenester for å føre regnskap for utdelte midler i forbindelse med komitéens opphør etter en kort periode. Ytes tjenesten pro forma vil det fortsatt skje i profesjonell kapasitet, men tjenesteavtalen kan begrenses i tid til den korte perioden det er behov. Slik vil det trolig ikke etableres et kundeforhold etter AMLD4.

Et annet unntak kan tenkes i det tilfelle regnskapstjenestene tilbys personer som ikke er bokføringspliktig, og kun har behov for hjelp med levering av skattemeldingen. Skattemeldingen leveres en gang i året og det kan dermed for en slik tjeneste tenkes et unntak. Er det videre tale om en enkeltlisens, og ikke et løpende abonnement, vil det trolig kreves noe mer for å kunne anføre at det foreligger et kundeforhold mellom den opplysningsfullmektige og personen.

Kontoopplysningstjenester kan også tilbys som en tredjepartstjeneste til leverandører med eksisterende kundeforhold.

[113] Ibid.

Man kan for eksempel tenke seg det tilfellet hvor en dagligvarekjede har vunnet en pristest, og er en gitt prosentandel rimeligere enn nummer to. Butikkjeden blir da kunde hos en opplysningsfullmektig som har konsesjon og en teknologisk plattform for å kunne tilby kontoopplysningstjenester. Den opplysningsfullmektige blir da mellomledd mellom butikkjeden og kontoeier. Den opplysningsfullmektige henter ut kontoopplysningene, og via deres teknologiske plattform, sorterer ut og leverer transaksjonsdata fra dagligvarebutikker til butikkjedens app, som så illustrerer hvor mye kontoeier hadde spart, om man gjorde all handlingen hos butikkjeden.

Den opplysningsfullmektige vil trolig ikke ha kundeforhold til kontoeier i dette tilfellet. Tjenesten har trolig ikke nytteverdi for kontoeier over tid, ettersom dagligvareprisene stadig endrer seg, og en pristest er slik mer et øyeblikksbilde enn en etablert sannhet.

Hvorvidt den opplysningsfullmektige har et kundeforhold til butikkjeden, er et mindre klart spørsmål og vil trolig bero på den tekniske integrasjonen av tjenesten. Tilbyr fullmaktforetaket et programvaregrensesnitt til butikkjeden, vil det kunne tale for at det foreligger et kundeforhold ettersom butikkjeden slik nyttegjør seg av fullmaktforetakets betalingstjeneste. Er fullmakttjenesten derimot drevet fra fullmaktforetakets plattform, og kun nyttegjort gjennom for eksempel en iframe, vil det trolig ikke foreligge kundeforhold til butikkjeden heller.[114]

5.2.3 Kundeløs tjeneste

Også der hvor kontoopplysningstjenestene tilbys direkte til kontoeier fra den opplysningsfullmektige, vil det ikke alltid foreligge et kundeforhold til kontoeier. Et eksempel er når en opplysningsfullmektig tilbyr kontoeiere å måle sitt forbruk opp mot SIFO-tallene. Om tjenesten kun tilbys i nettleseren, og informasjonen ikke lagres, slik at når nettleseren lukkes, forsvinner også all informasjon, vil det heller ikke her foreligge et kundeforhold etter AMLD4.

Også betalingsfullmektiger kan befinne seg i situasjoner hvor de trolig ikke etablerer kundeforhold. I det tilfellet hvor en markedsplass for brukthandel mellom privatpersoner, tilbyr betalingsinitieringstjenester til brukerne for oppgjør seg imellom, kan omstendighetene tale for at det ikke etableres kundeforhold, verken til betaler eller betalingsmottaker.

Om Peder Ås initierer en betaling via en markedsplass til Marte Kirkerud for en antikk bakebolle, er det ingenting som tilsier at Peder og Marte har inngått et forhold som er forventet å vare over tid. Opprettelse av én annonse for én antikk bakebolle én gang, eller kjøp av en slik gjenstand én gang, vil trolig heller ikke være et forhold som er forventet å vare over tid. Slik vil det også kunne anføres at det ikke etableres et kundeforhold mellom Marte og markedsplassen eller Peder og markedsplassen.

[114] Om iframe, se Stenseth (2014)

Om markedsplassen ikke krever opprettelse av konto for noen av partene, men kun opptrer som en teknisk tilrettelegger, vil dette tale ytterligere for et slikt utfall.

5.2.4 Oppsummering

Det er altså med dette klart at kundeforhold vil bero på en konkret vurdering av hovedsakelig AMLD4 sitt andre kumulative vilkår om hvorvidt forholdet er forventet til å vare over tid. Det er også klart at dette ikke alltid vil kunne gjøres gjeldende for kontoeier. Videre er det klart at fullmakttjenester kan tilbys uten at det etableres kundeforhold til hverken kontoeier eller en annen part. Med dette som bakteppe vil jeg nå drøfte anti-hvitvaskingspliktene presentert i forrige kapittel i lys av PSD2.

5.3 Risikovurderinger

Risikovurdering er inngangsporten til anti-hvitvaskingsarbeidet. Det er også trolig et implisitt krav om risikovurdering i PSD2. Betalingsinstitusjoner som er underlagt anti-hvitvaskingsregelverket, skal ved konsesjonssøknad inkludere anti-hvitvaskingsrutiner.[115] Slik er også kravet overlappende med det som stilles i AMLD4, hvor anti-hvitvaskingsrutiner etableres på bakgrunn av risikovurderinger. Det kan slik anføres at det indirekte foreligger et krav, også i PSD2, om at fullmaktforetak skal gjøre risikovurderinger for slik å kunne etablere anti-hvitvaskingsrutiner. Et spørsmål blir da hva risikovurderingene skal omfatte.

Risikovurdering både av virksomheten, produktene og tjenestene skal gjøres selv av et fullmaktforetak som ikke har kundeforhold. En opplysningsfullmektig vil i likhet med betalingsfullmektig heller ikke utføre transaksjoner, og vil derfor ikke ha behov for å risikovurdere enkelttransaksjoner. Hva som i disse tilfellene skal risikovurderes av den opplysningsfullmektige, er uklart.

Et generelt krav om risikovurderinger, uavhengig av valg av forretningsmodell, fremstår som betenkelig i lys av formålet om å sikre tilgang til nye aktører etter PSD2 “regardless of the business model applied by them”.[116] Reglene for risikovurdering fremstår særlig for opplysningsfullmektiger som mindre klar, i strid med PSD2 sin ambisjon om et “clear [...] regulatory framework”.[117]

Økte regulatoriske krav på private tjenestetilbydere, vil ofte resultere i høyere kostnader for sluttbruker. Krav om risikovurderinger fra fullmaktforetakene, uten tilpasninger som hensyntar deres særegne stilling i betalingskjeden, vil slik også kunne anføres å komme i strid med PSD2 sitt formål om å styrke forbrukernes rettigheter. Fullmaktforetak ble introdusert nettopp for å styrke

[115] PSD2, artikkel 5, bokstav K
[116] PSD2, fortalen, avsnitt 33
[117] Ibid.

konkurransen til forbrukernes gunst. Den økonomiske begunstigelsen kan fort fordufte i møte med regulatorisk iver.

I det videre vil jeg kort kommentere de ulike produkt- og tjenesterisikoene som ble presentert i forrige kapittel.

5.3.1 Kombinerte transaksjoner

En av de innovative betalingstjenestene en betalingsfullmektig kan tilby, er som tidligere vist kombinerte transaksjoner hvor flere kontoer trekkes på betalers side, for en samlet overføring til betalingsmottaker.

Dette vil imidlertid ikke kunne anføres som en produkt- eller tjenesterisiko. Ettersom den betalingsfullmektige ikke deltar i å utføre betalingsoverføringer, vil heller ikke den betalingsfullmektige være rapporteringspliktig på dette grunnlaget. Og har ikke den betalingsfullmektige et kundeforhold til kontoeieren som hvitvasker, er den heller ikke rapporteringspliktig for forholdet etter reglene i AMLD4.

Imidlertid er også et høyt antall mindre beløp også et risikomoment som kontotilbydere er oppmerksom på. En hvitvasker vil derfor måtte ha et svært høyt antall kontoer hos et tilsvarende antall kontotilbydere, og samtidig ha et system for å få penger inn på disse, for å kunne utnytte kombinerte transaksjoner i en skala som vil være av betydning. Dette medfører betydelig arbeid, og er derfor trolig ikke en attraktiv hvitvaskingsmetode.

5.3.2 Mannen-i-midten-angrep

En annen produkt- og tjenesterisiko som har blitt trukket frem i teorien for fullmaktforetak, er det tilfellet hvor et fullmaktforetak passivt eller aktivt medvirker til hvitvasking.

Risikoen for mannen-i-midten-angrep begrenses både av betalers og betalingsmottakers kontotilbyderes anti-hvitvaskingsrutiner, og av at betalingsinitieringstjenester er konsesjonsbelagt og slik har en hindring for misbruk.

Mannen-i-midten-angrep er også en risiko som vil løpe for alle typer tjenester hvor to parter samhandler, og er ikke begrenset til nett. Tilfeller av mannen-i-midten-angrep forekommer også i kortterminaler i fysiske butikker og i minibanker.[118]

[118] Akter et. al. (2020)

Samtidig er trolig det potensielle skadeomfanget for en betalingsfullmektig nærmere andre betalingstjenestetilbydere, enn en enkelt kortterminal. En annen faktor er at fysiske angrep vil kreve fysisk tilstedeværelse, mens et digitalt angrep med en betalingsinitieringstjeneste, i prinsippet kan utføres hvor som helst i verden.

5.3.3 Automatisert hvitvasking

Den tredje produkt- og tjenesterisikoen, er faren for at en fullmakttjeneste blir misbrukt til automatisert hvitvasking.

All aktivitet fra fullmakttjenester vil logges av både fullmaktforetaket selv og kontotilbyderen.[119] Derfor vil misbruk av en fullmakttjeneste til hvitvasking bety at en hvitvasker legger igjen store mengder digitale fotavtrykk en etterforskning senere kan nyttegjøre. Automatisert hvitvasking vil derfor fordre tilgang på et høyt antall fullmaktforetak for at fordelen skal være større enn ulempen for en hvitvasker.

Automatisert hvitvasking vil også trolig være begrenset på grunn av fullmaktforetakenes natur; de er relativt sett mindre, har større grad av nisjepreg og står relativt sett for lave volum. Hvitvaskere vil i tilsløringsprosessen være avhengig av det motsatte, og vil effektivt sett ønske å skjule seg i mengden. Dette vil derfor representere betydelige ulemper for en hvitvasker, og begrense pengemengden som kan vaskes gjennom strukturer som bygger på fullmaktforetak.

5.4 Kundetiltak

Den andre anti-hvitvaskingsplikten som ble utredet i det forutgående kapittelet, var kundetiltak. Som vist, utløses kundetiltak som risikovurdering ved stiftelse av kundeforhold, men skal også ha form som en løpende overvåkning av kundeaktiviteten.

Ved stiftelse av kundeforhold hvor kunden er en naturlig person, vil det som hovedregel være tilstrekkelig med forenklede kundetiltak, og dette sammenfaller med kravet om sterk kundeautentisering i PSD2. Forenklede kundetiltak vil kunne basere seg på identitetsbekreftelse gjennom kontoeierskap. Det vil derfor kunne anføres at forenklede kundetiltak når de stifter kundeforhold til naturlige personer, har en plikt som er proporsjonal med PSD2. Problemet oppstår i de tilfellene hvor det er krav om noe mer enn forenklede kundetiltak. Spørsmålet blir da, når vil ikke forenklede kundetiltak være tilstrekkelig?

En typisk høyrisikosituasjon for fullmakttjenester er ved kundeforhold til en PEP.[120]

[119] PSD2, artikkel 21
[120] Se 4.3 om kundetiltak

Ved kundeforhold til PEP, skal alltid forsterkede kundetiltak gjennomføres. Betalingsforetak har ikke anledning til å avvise PEP på grunnlag av at de er PEP. Avvisning av en transaksjon eller et kundeforhold, må bero på en konkret vurdering og være objektivt begrunnet.[121]

Et annet tilfelle hvor det er nødvendig med mer enn forenklede kundetiltak, er når kunden er en juridisk person. Det gis ingen anvisninger om forenklede kundetiltak er tilstrekkelig.

Fordi det uansett er krav om avklaring av reelt eierskap ved juridiske personer som kunder, vil de totale pliktige undersøkelsene ved kundeforholdet få et omfang utover forenklede kundetiltak.

Et slikt generelt krav om ytterligere kundetiltak utover forenklede for opplysningsfullmektiger synes å være uproporsjonal med tjenesterisikoen. Et typisk eksempel på en kontoopplysningstjeneste brukt av selskaper, er import av kontotransaksjoner til sitt regnskapsprogram. Hvilken merrisiko for hvitvasking som oppstår ved at kontotransaksjonene importeres direkte til regnskapsprogrammet, versus andre løsninger, er vanskelig å se.

For betalingsfullmektiger vil dette stille seg nokså likt. Et typisk eksempel på en betalingsinitieringstjeneste er en nettbutikk som tilbyr kundene å betale med betalingsinitiering som et alternativ til kortbetaling. I dette tilfellet vil nettbutikken da være betalingsmottaker og den betalingsfullmektiges kunde. Det kan da anføres at et strengere krav vil være mer proporsjonalt for en betalingsfullmektig enn i det forutgående tilfellet som gjaldt en opplysningsfullmektig.

Fordi en betalingsfullmektig aldri holder kundemidler, og ikke selv er den som utfører transaksjonen, vil det likevel synes uproporsjonalt. Betalers, nettbutikkundens, kontotilbyder og betalingsmottakers, nettbutikkens, kontotilbyder, vil begge uansett være pliktige å både risikovurdere kundeforholdene og utføre løpende kundetiltak. Det var aldri intensjonen at fullmaktforetak skulle fungere som en oppsynsmann for kontotilbyder. Det er kontotilbyder som er best egnet til å være betalingssystemets portvoktere, og der hvor et fullmaktforetak misbrukes til hvitvasking, vil alltid betalingstjenestene til kontotilbyder utnyttes likt.

Pulveriseringshensynet taler også for en slik løsning. Det er kontotilbyder som har størst mulighet til å pulverisere de økonomiske kostnadene som følger av anti-hvitvaskingsarbeidet. Betaler kan gjennomføre betalinger uten en betalingsfullmektig, men vil motsatt aldri kunne bruke en betalingsinitieringstjeneste uten å ha en konto å initiere betalingen fra. Transaksjonene kan

[121] AMLD4, fortalen, avsnitt 33

gebyrlegges med for eksempel transaksjonsgebyr og valutapåslag, og kontotilbyder kan tjene penger på utlån av innskudd på kontoen mellom overføringene.

Dette samstemmer også med prinsippet i PSD2 om den erstatningsrettslige ansvarsdelingen mellom betalingsfullmektig og kontotilbyder; "the allocation of liability [...] should compel them to take responsibility for the respective parts of the transaction that are under their control".[122]

Dermed kan trolig samme prinsipp anføres for fullmaktforetakene. Fordi man må ha et kundeforhold til en kontotilbyder for å kunne bruke en fullmakttjeneste, og betalingstjenesten alltid må gjennomføres av kontotilbyder, ikke fullmaktforetaket, vil det alltid være slik at kontotilbyder er pliktig å utføre de samme anti-hvitvaskingspliktene som fullmaktforetaket.

Et videre spørsmål er hvilke praktiske muligheter fullmaktforetak har til å utføre kundetiltak.

Betalingsfullmektig har ikke tilgang på andre overføringer enn den de selv initierer. En hvitvasker som initierer flere betalingsoverføringer fra ulike betalingsfullmektiger fra samme konto, vil slik ikke bli oppdaget av noen av dem. Kontotilbyder vil imidlertid ha full innsikt i aktiviteten.

Opplysningsfullmektig har ikke tilgang på betalingsmottakers internasjonale bankkontonummer (IBAN) eller bankenes identifiseringskode (BIC). Dermed vil ikke en opplysningsfullmektig kunne skille ulike transaksjoners betalingsmottakere fra hverandre, eller bestemme den geografiske risikoen til betalingsmottakers kontotilbyder. En opplysningsfullmektig vil slik ikke kunne gjennomføre løpende kundetiltak. På tross av dette er fullmaktforetakene for sine kundeforhold pålagt å utføre selvstendige kundetiltak i henhold til AMLD4.

Et neste spørsmål blir da hvordan dette står seg i lys av formålene i PSD2 i henhold til oppgavens hovedspørsmål. For å svare på det, er det først nødvendig å vurdere de faktiske følgene av kundetiltakene for fullmaktforetakene. Er de av mindre belastning, vil det være mindre begrensende for nye aktører og medføre mindre kostnader. Er de av større belastning, vil det være begrensende, i ytterste konsekvens også for innovasjon og utvikling av nye tjenester.

Ettersom risikoen for fullmaktforetak er begrenset, er utgangspunktet forenklede kundetiltak. Ved forenklede kundetiltak er det tilstrekkelig med verifisering av kundens navn, og identiteten kan bekreftes med kontoeierinformasjon.[123]

[122] PSD2, fortalen, avsnitt 74
[123] EBA/GL/2021/02, s. 128-129

I de tilfellene hvor fullmaktforetakets kunde er betaler og forenklede kundetiltak er tilstrekkelig, vil kundetiltakene kunne gjennomføres samtidig med betalingsgjennomføringen. PSD2 forutsetter bruk av sterk kundeautentisering når en kontoeier enten bruker en betalingsinitieringstjeneste eller en kontoopplysningstjeneste.[124] Slik vil kostnaden med kundetiltakene være begrenset for tilfellene hvor forenklede kundetiltak er tilstrekkelig.

Forsterkede kundetiltak vil i liten grad være mulig å automatisere fullstendig, ettersom fullmaktforetakene må "obtain senior management approval for establishing or continuing business relationships with such persons".[125]

Igjen er det nødvendig å minne om fullmaktforetakenes særegne stilling: For å kunne benytte seg av tjenestene til et fullmaktforetak, må man allerede ha et kundeforhold til et kontotilbydende betalingsforetak. Kontotilbyder vil allerede ha gjort et forsterkede kundetiltak av kontoeiere som er PEP, og er pålagt særlige rutiner for overvåkning av kundeforholdet generelt og transaksjoner spesielt.

Forsterkede kundetiltak vil være kostnadsdrivende. Slik vil krav om forsterkede kundetiltak svekke fullmaktforetakenes konkurranseevne i møte med andre betalingstjenester, som for eksempel kortbetaling.

5.5 Reelt eierskap

Den tredje anti-hvitvaskingsplikten som ble utredet i det forutgående kapittelet, var plikten til å avklare reelt eierskap.

Avklaring av reelt eierskap henger som nevnt sammen med kravet om kundetiltak, og formålet er å avklare om det finnes en eller flere naturlige personer med eierskap eller innflytelse tilsvarende eierskap på mer enn 25%.

Avklaring av reelt eierskap er som poengtert i det forutgående om kundetiltak, lite relevant for opplysningsfullmektiger fordi det er praktisk umulig for dem å oppdage hvitvasking.

For betalingsfullmektig vil det samme kunne gjøres gjeldende, som drøftet i delkapittelet om kundetiltak. Betalingsfullmektig utfører ikke betalingen, men initierer den. Hvitvaskingsrisikoen synes å være den samme uavhengig av om en betaling initieres av kontoeier selv direkte i kontotilbyders nettløsning, eller om betalingen initieres via en betalingsfullmektig.

[124] PSD2, artikkel 97, bokstav a-b
[125] AMLD4, artikkel 20, bokstav b, punkt (i)

Utgangspunktet er imidlertid forenklede kundetiltak for fullmaktforetak. Ved forenklede foretak er det som minimum tilstrekkelig å kjenne kundens navn.[126] Slik faller dermed anti-hvitvaskingsplikten bort for de tilfellene hvor det er tale om lav kunderisiko.

Avklaring av reelt eierskap henger imidlertid sammen med reglene for PEP. En PEP som vil bruke et fullmaktforetak til å hvitvaske penger, vil kunne omgå kontroll ved å utføre transaksjonene via en juridisk person. Selv om juridiske personer hvor PEP utøver reelt eierskap stiller likt med en naturlig PEP, vil det uten krav om kontroll av reelt eierskap trolig ikke avdekkes om en virksomhet har en eller flere reelle eiere som er PEP, om ikke kunden selv opplyser om det eller gir opplysninger om andre forhold som utløser krav om strengere tiltak.

Dermed kan det anføres at kravet om forsterkede kundetiltak for naturlig personer som er PEP, blir meningsløst all den tid kravet kan omgås ved å gå via en juridisk person, og ikke opplyse om sitt reelle eierskap.

Imidlertid vil det samme rasjonale som ved kundetiltak presenteres. Fullmaktforetak er ikke selv portvoktere til det finansielle systemet, men er begrenset til en tredjepartsleverandør som hekter seg på det eksisterende betalingssystemet. Dette har negative sider som fravær av eierskap til infrastruktur og et indirekte avhengighetsforhold til kontotilbydere, men også positive sider, som å kunne gjøre forenklede kundetiltak ved å ta utgangspunkt i at kontoeierskap i seg selv er en legitimasjon.

Betalingsfullmektigenes konkurrent er uansett primært kortnettverkene, som ikke er underlagt anti-hvitvaskingspliktene i AMLD4 i forholdet til kontoeier. Dette står i kontrast til de faktiske forholdene. Kortnettverk utfører overføringer, betalingsfullmektiger initierer kun. Betalinger utført via kortnettverk kan gå via flere en rekke kontoer holdt hos ulike kontotilbydere, før den når betalingsmottaker. Betalinger initiert via en betalingsfullmektig vil alltid gå direkte fra betaler til betalingsmottaker.[127] Å nøste opp i hvem som betalte hvem, hva, når, kan altså være betydelig enklere ved betalinger initiert via en betalingsfullmektig, enn betalinger utført via et kortnettverk.

5.6 Rapporteringsplikt

Fullmaktforetakene har også rapporteringsplikt. Spørsmålet er hva fullmaktforetakene skal sende MT-meldinger om.

Fullmaktforetak har i utgangspunktet et svært avgrenset forhold til betaler, sammenlignet med det forholdet som for eksempel er mellom en bank og dens kunde. Fullmaktforetakenes kundetiltak

[126] EBA/GL/2021/02, s. 128
[127] Olsen (2021)

bygger som tidligere vist på bankenes kundetiltak ved at kontoeierskapet i seg selv fungerer som en legitimering ved stiftelse av kundeforholdet. Og for fullmaktforetak som tilbyr kundeløse tjenester, vil det heller ikke være et kundeforhold å rapportere om.[128]

Dermed oppstår et betimelig spørsmål: Hva er nytteverdien av rapporteringsplikten for fullmaktforetak? I motsetning til tradisjonelle betalingstjenestetilbydere som ofte har filialer i statene de driver virksomhet i, og slik har rapporteringsplikt, vil fullmaktforetak som kun er fullmaktforetak som hovedregel ikke ha filial eller på annen måte rapporteringsplikt til andre enn FIU i hjemstaten.

At heller ikke kortnettverkene, betalingsfullmektiges hovedkonkurrenter, er pålagt rapporteringsplikt, er til skade for konkurransen, og slik trolig i strid med formålet i PSD2 om rettferdig konkurranse mellom alle betalingstjenestetilbydere.

6 Konklusjon

I oppgaven har jeg undersøkt hvorvidt det foreligger en faktisk motstrid mellom formålene i PSD2 og pliktene i AMLD4 for fullmaktforetak. Problemstillingen er vurdert ved å presentere formålene i PSD2, og deretter pliktene i AMLD4, for så å sammenholde pliktene i AMLD4 enkeltvis opp mot formålene i PSD2.

For det første er det i oppgaven påvist at regelverket slik det står i dag, ikke har tatt høyde for de tilfellene hvor fullmaktforetak ikke har kunder, slik kundeforhold er definert i AMLD4. Dette skaper en rettslig usikkerhet for denne type fullmaktforetak, som kolliderer med formålet i PSD2 om en rettslig harmonisering til gunst for konkurransesituasjonen og innovasjonsevnen til europeiske foretak.

Verken direktivenes forarbeid, direktivenes fortaler, direktivtekstene eller etterarbeid, gir anvisning på tilfellene hvor fullmaktforetak som tilbyr fullmakttjenester, ikke har kundeforhold.

For det andre er det i oppgaven påvist at regelverket ikke forskjellsbehandler fullmaktforetak og kontotilbyder i spørsmålet om undersøkelsesplikt og påfølgende rapportering. I forlengelsen av dette påvises det i oppgaven at det sjelden er slik at et fullmaktforetak vil være rapporteringspliktig for et forhold som kontotilbyder ikke er. I praksis gjør dette fullmaktforetakets rapporteringsplikt formålsløs.

[128] Se kapittel 5.2.3 om kundeløse tjenester

Oppgaven viser at pliktene samlet sett, og undersøkelses- og rapporteringsplikten i særlig grad, er ressurskrevende. Dette medvirker indirekte til mindre innovasjon og mindre konkurranse, og slik indirekte høyere priser og dårligere tjenester. Slik representerer dette også en samfunnskostnad. Et slikt pålegg overfor fullmaktforetakene bør derfor gi en faktisk verdi for samfunnet. Litt banalt sagt, kan man si at slik regelverket står i dag, vil den eneste effekten av å fjerne rapporteringsplikten for fullmaktforetak helt, være at det genereres et lavere antall MT-meldinger.

Den andre slagsiden av dette, overrapportering, har også en naturrettslig karakter. Takáts bruker historien om gutten som ropte ulv for å beskrive situasjonen, og anfører at de rapporteringspliktige får et incentiv for å overrapportere, heller enn aktivt ta stilling til hva som er mest aktuelt for FIU å vurdere.[129] Dilemmaet som oppstår da, er til forveksling lik fangens dilemma. Rapporterer den rapporteringspliktige for lite, vanker det potensielt få strafferettslige konsekvenser. Rapporterer den rapporteringspliktige for mye, får det ingen konsekvenser. For samfunnet kan det derimot få store konsekvenser. Rui påpeker at kvalitetsproblemene ved MT-meldingene vanskeliggjør arbeidet til FIU.[130] Overbelastningen reduserer effektiviteten til anti-hvitvaskingsarbeidet.[131] Norske myndigheter har påpekt nettopp overbelastningen som en utfordring som følge en asymmetrisk oppbemanning hos de rapporteringspliktige i disfavør av myndighetene.[132] Slik får hvitvasking, og kriminaliteten den finansierer eller incentiverer, pågå lengre enn nødvendig.

Et eksempel på det siste, en av de såkalte Darkroom-sakene i Norge. Darkroom-sakene gjelder nettbaserte seksuelle overgrep mot barn. I en av sakene ble en norsk mann dømt for å ha begått overgrep via nett mot omkring 190 mot barn under 14 år og under 16 år på Filippinene mellom 2012 og oktober 2016.[133] Overgrepene ble utført med penger som virkemiddel. Overføringene ble utført via minst fire ulike betalingstjenestetilbydere. Minst to av disse sendte MT-meldinger som følge av utestengelse etter mistenkelige overføringer; først i 2012, deretter i 2014. Minst tre av betalingstjenestetilbyderne som ble brukt har ikke rapportingsplikt til FIU i Norge.

For det tredje er det i oppgaven påvist at fullmaktforetak som hovedregel kun vil være rapporteringspliktig til FIU i hjemstaten. Fullmaktforetak som kun har konsesjon som fullmaktforetak, har ikke filialer og vil sjelden ha stedlig representasjon utenfor hjemstaten som utløser rapporteringsplikt til en vertsstat som ikke er hjemstaten. Sammenholdt med avsnittet ovenfor, understreker dette de faktiske utfordringene med regelverket.

[129] Takáts (2011), s. 33-36
[130] Rui (2012), s. 243
[131] Takáts (2011), s. 34
[132] NRA, 2020, side 33, punkt 3.7.5
[133] TBERG-2018-51923

Det kan videre anføres at regelverket slik det står i dag hva gjelder rapporteringsplikt for fullmaktforetak, i beste fall er et sikkerhetsteater, og i verste fall er med å svekke det europeiske anti-hvitvaskingsarbeidet. Rapporteringsplikten er til den enkelte FIU i den enkelte stat, hvor fullmaktforetaket er hjemmehørende. Rapporteres det, vil MT-meldingen først etter en vurdering av FIU i hjemstaten eventuelt bli videresendt, etter oversettelse, til FIU i kontoeiers hjemstat. Ulike krav til hva det skal rapporteres om, når det skal rapporteres og en forlenget rapporteringsprosess, svekker statenes mulighet til å få opplysninger om potensiell kriminalitet.

Kombinasjonen av etableringsfriheten, AMLD4s hjemstatsprinsipp, og at fullmakttjenester alltid er digitale, ikke bare åpner opp for, men gir et tydelig incitament til gründere om å vurdere kostnadene til anti-hvitvaskingsarbeid ved valg av selskapsjuridiksjon. Trolig vil andre faktorer veie tyngre, likesom at alle europeiske selskaper som ikke har et fast forretningssted ikke er etablert på Malta med effektiv selskapsbeskatning på 5% vs. EU-gjennomsnittet på 21,9%.[134] Normalt sett vil det kunne blitt anført at en slik konkurranse mellom statene ikke bare er sunn, men nødvendig for å drive frem konkurransefordeler, og at samlet sett er det til netto begunstigelse fordi europeiske stater konkurrerer like mye globalt som kontinentalt om de store pengene og de store arbeidsplassene. For anti-hvitvaskingsarbeidets del, vil dette imidlertid havne i skyggen av kriminalitetens kostnad. Anti-hvitvaskingsarbeid reduserer ikke bare omfanget av og incitamentet til skatteunndragelse og korrupsjon, men også annen alvorlig kriminalitet som seksuelle overgrep mot barn og narkotikakriminalitet.[135]

For det fjerde er det i oppgaven påvist at fullmaktforetak er pålagt å utføre forsterkede kundetiltak i tilfeller hvor det er høy risiko tilknyttet kundeforholdet.

Reglene for kundetiltak i AMLD4 for fullmaktforetakene er begrensende for fullmaktforetakenes mulighet til fritt å tilby fullmakttjenester i EØS-området.

Reglene for kundetiltak krenker også forbrukernes valgfrihet ved at de vil pålegges dobbeltkrav i tilfeller hvor risikoen vurderes som høy, for eksempel på bakgrunn av status som PEP.

Det fremstår også noe inkonsekvent å vurdere den generelle hvitvaskingsrisikoen for fullmaktforetakene som lav på grunn av virksomhetenes natur og manglende rolle i betalingssystemet, men samtidig anvende det samme regelverket for PEP som brukes av betalingsforetak som gjennomfører transaksjoner.

[134] KPMG (2019); Asen (2021)
[135] Grimstad (2019); Politidirektoratet & Politiets sikkerhetstjeneste (2020) s. 18-21

All den tid ingen fullmakttjenester kan tilbys av et fullmaktforetak, uten å gå via minst ett annet kontotilbydende betalingsforetak, fremstår det betenkelig. Grunntanken om at kontoeierskap i seg selv er en legitimasjon for bruk av lavrisikobetalingstjenester som betalingsinitieringstjenester og kontoopplysningstjenester, får ikke skje fyllest.

Kundetiltakskravene til fullmaktforetakene vil også kunne komme i motstrid med reglene for finansiell inkludering og kontraheringsplikt. Sårbare gruppers tilgang til nye finansielle tjenester vil i praksis begrenses av at de oftere enn andre blir vurdert med høy kunderisiko. Satt på spissen vil for eksempel en asylsøker risikere å måtte sende inn fødselsattest og pass hver gang hen skal handle på nett, på tross av at hen trolig har gjennomgått grundige kundetiltak for å kunne opprette konto hos en kontotilbydende betalingstjeneste i EØS-området.

For det femte er det i oppgaven påvist at fullmaktforetak som hovedregel er avhengig av tredjepartsleverandører for å kunne oppfylle pliktene i AMLD4.

Europol har foreslått mer bruk av private tjenesteleverandører.[136]

Tredjepartsleverandører representerer en terskel for nye aktører ved at innovasjonen begrenses til å befinne seg innenfor rammene av leverandørsystemene. Nye fullmakttjenester vil slik i ytterste konsekvens ikke kunne realiseres. En høyere terskel for nye aktører, vil få utslag i mindre innovasjon og dårligere utvalg av tjenester og produkter for forbrukerne.

Den franske bransjeorganisasjonen for fullmaktforetak har også argumentert for et klimarettslig perspektiv på bruken av tredjepartsleverandører.[137] Tredjepartsleverandørene er avhengig av å bruke maskinlæring for å identifisere avvikende forhold. Det er en betydelig klimakostnad tilknyttet maskinlæring.[138] Dermed blir det aktuelt å vurdere hvorvidt bruken er nødvendig, sett i lys av klimakostnadene. Med tanke på den rettslige utviklingen i klimaspørsmål, er dette et perspektiv som trolig vil få større vekt i tiden fremover.

I problemstillingen stilte jeg en hypotese, og jeg finner det derfor nødvendig å trekke en mer konklusiv slutning som tilsvar til den. Basert på det forutgående og de tidligere kapitlene, har jeg kommet frem til at det foreligger en delvis faktisk motstrid mellom formålene i PSD2 og pliktene i AMLD4.

[136] European Police Office (2017) s. 37 og 39
[137] AFEPAME (u.å.)
[138] Dhar (2020)

Rettsklarheten for fullmaktforetak, et av primærformålene stilet i PSD2, er på anti-hvitvaskingsregelverkets område ikke klart.

Fullmaktforetakene pålegges en rekke anti-hvitvaskingsplikter, uten at de medfører en klar merrisiko. Slik fremstår restriksjonene som følger av AMLD4, uproporsjonal med formålene i PSD2.

Den delvis faktiske motstriden forsterkes trolig gjennom nasjonale regler for anti-hvitvasking. Strengere krav vil ofte gi et mer urimelig utfall for fullmaktforetak.

Slik egner også oppgavens tema seg godt for videre forskning. Pliktene i AMLD4 er minimumskrav som gir anledning til nasjonale tilpasninger, mens PSD2 er fullharmonisert og skal gjelde likt i hele EØS. Her foreligger det en ytterligere kilde til motstrid mellom nasjonal rett og PSD2. I hvor stor grad kan nasjonal rett pålegge fullmaktforetak anti-hvitvaskingsplikter, uten å skape motstrid mellom nasjonal rett og formålene i PSD2? Og videre: I hvor stor grad kan nasjonal rett pålegge fullmaktforetak anti-hvitvaskingsplikter som i praksis vanskeliggjør betalingstjenestevirksomhet utenfor hjemstaten i lys av betalingsforetaks kontraheringsplikt og det EU-rettslige ikke-diskrimineringsprinsippet?

Jeg vil understreke at løsningene som er presentert, er enda usikre. Den EU-rettslige rettstilstanden på anti-hvitvaskingsområdet er i rivende utvikling, og AMLD4s arvtaker, AMLD5, har allerede trådt i kraft i EU og er til vurdering for innlemmelse i EØS-avtalen.[139] Industrien har allerede begynt å drøfte AMLD6. Likesom er det ventet et nytt betalingstjenestedirektiv, et PSD3.[140] Det vil også være behov for betydelig forskning på området, etterhvert som fullmakttjenester utbres i omfang, og tas i bruk av flere aktører i flere sammenhenger.

Jeg avgrenset oppgaven til direktivene, og har ikke kommentert norsk rett. Det er likevel verdt å poengtere at slik regelverket står i dag, er det flere uklarheter hva gjelder norsk implementering. Finanstilsynets veileder til hvitvaskingsloven gir liten veiledning for fullmaktforetak. Det er per i dag kun 3 av 21 betalingsforetak som kun har konsesjon til å tilby fullmakttjenester hjemmehørende i Norge.[141] Det tilsvarende tallet for Tyskland er 15 av 64.[142] Om rettsuklarheten har medvirket til det relativt lave tallet i Norge, vites ikke.

[139] Directive (EU) 2018/843
[140] Eroglu (2018)
[141] Finanstilsynet (2020)
[142] Bundesanstalt für Finanzdienstleistungsaufsicht (u.å.)

7 Rettspolitiske betraktninger

I oppgaven, senest i konklusjonen i forrige kapittel, er det påvist en dissonans mellom regelverket i PSD2 og regelverket i AMLD4 for fullmaktforetak.

Som skissert i oppgavens innledning, ønsker jeg derfor å runde av med noen rettspolitiske betraktninger.

Med bakgrunn i konklusjonen som ble gitt i det forutgående kapittelet, synes det klart at det er behov for et anti-hvitvaskingsregime som i større grad tar høyde for de særskilte utfordringene som følger av fullmaktforetakenes betalingstjenestevirksomhet. Dette åpner opp for å ta et skritt tilbake og se regelverket an i et mer holistisk perspektiv med utgangspunkt i spørsmålet: Hvordan burde regelverket vært for å sikre oppfyllelsen av AMLD4 på en måte som ikke begrenser fullmaktforetakene i en slik grad at det kommer i strid med formålene i PSD2?

I det videre vil jeg prøve å ta sikte på presentere en mulig løsning på dette spørsmålet.

En mulig løsning ville være å bygge fullmaktforetakenes rett på et avtaleforhold til kontotilbyder, for så å utnytte muligheten for informasjonsdeling i AMLD4 slik at fullmaktforetakene begrenser seg til å varsle kontotilbyder.[143] En slik løsning er klart i strid med regelverket i PSD2, og vil gå på tvers av grunntanken om fullmaktforetakenes uavhengighet fra kontotilbyder.[144] Rent praktisk vil det også trolig åpne opp for en rekke rettslige spørsmål ved innføring i nasjonal rett, og slik være til hinder for den rettslige harmoniseringen og i ytterste konsekvens stille utviklingen av europeisk finansteknologi i bero.

Prinsippet har kanskje likevel livets rett. Det har trolig noe for seg å i større grad enn i dag å holde kontotilbyder ansvarlig som portvokter. Det er kontotilbyder som har kundeforholdet til en kontoeier som vasker penger eller finansierer terror, som trolig har best forutsetninger for å oppdage mistenkelig aktivitet.

Det eksisterer også allerede en sikker kommunikasjonslinje mellom fullmaktforetak og kontotilbyder. I dag går kommunikasjonen én vei, fra kontotilbyder til fullmaktforetak. Det vil trolig kreve få endringer i personvernregelverket for å tillate en slik kommunikasjon. Nødvendig databehandling som følge av EU-rett eller nasjonal rett er allerede gyldig behandlingsgrunnlag etter General Data

[143] AMLD4, artikkel 39 (5)
[144] PSD2, artikkel 66 (5); artikkel 67 (4)

Protection Regulation (GDPR) og behandlingsgrunnlaget som brukes for utførelsen av anti-hvitvaskingspliktene.[145]

Som påpekt i oppgavens forutgående kapitler, er riktignok en av hovedutfordringene for fullmaktforetakene det manglende informasjonsgrunnlaget de ofte vil ha, og fraværet av kundeforhold å behandle informasjon på grunnlag av.

Fullmaktforetakene vil imidlertid kunne tilføre den informasjonen kontotilbyder selv går glipp av ved bruk av fullmakttjenester versus kontotilbyders egne betalingstjenester, for eksempel informasjon om betalingsoverføringens formål, betalingsmottaker, med mer. Fordi kontotilbyders behandlingsgrunnlag for denne informasjonen er begrenset til å gjennomføre lovpålagte anti-hvitvaskingsplikter, vil det også i liten grad representere en kommersiell trussel for fullmaktforetakene å dele slike brukerdata.

Kontotilbyder på sin side vil kunne dra nytte av denne ekstra informasjonen for å spore mistenkelige avvik, for eksempel det tilfellet hvor betaler oppgir to ulike formål for overføringen eller to ulike betalingsmottakere til henholdsvis fullmaktforetaket og kontotilbyder.

Et generelt problem for anti-hvitvaskingsarbeidet slik det står i dag, er de spillteoretiske utfordringene dagens regelverk fremtvinger.[146] Å pålegge fullmaktforetakene en informasjonsdelingsplikt med kontotilbyder for anti-hvitvaskingsformål som et alternativ til dagens system, er et riktig skritt til i større grad å kunne samordne aktørenes interesser til det beste for storsamfunnet, kundene og aktørene selv. En slik informasjonsdelingsplikt vil også være klart mindre tyngende og slik mer proporsjonalt med regelverket og formålene i PSD2 hva gjelder fullmaktforetakenes natur og tjenestetilbud. I stedet for å måtte drifte et betydelig anti-hvitvaskingsarbeid, vil fullmaktforetakene kunne helautomatisere innrapportering om brukeraktivitet uavhengig av kundeforhold til de respektive kontoeiernes kontotilbydere.

En mulig innvending er at dette på nytt vil være å pålegge kontotilbydere kostnader for å tilrettelegge for andre og nye kommersielle aktører. Igjen vil det være nødvendig å minne om kontotilbyders pulveriseringsmuligheter av disse kostnadene.[147] Videre er det nødvendig å minne om kontotilbyders privilegerte posisjon; det er i praksis ikke mulig å leve et liv uten å forholde seg til minst én kontotilbyder i det moderne samfunnet, og adgangen til å drive en slik virksomhet er svært begrenset. Det kan synes rimelig å dra en parallell til et annet allment gode driftet av private - telenettet. Tjenestene har til felles at de begge tjener et allmennyttig formål og er en del av den grunnleggende

[145] Regulation (EU) 2016/679; GDPR, artikkel 6 (4)
[146] Se kapittel 6
[147] Se kapittel 5.4 og kapittel 6

infrastrukturen i samfunnet. De er også begge strengt regulert og konsesjonsbelagt. Og der hvor teleselskap må bære utgifter til fysisk vedlikehold og drift, må kontotilbyder etterleve anti-hvitvaskingspliktene.

Parallellen synes også rimelig ettersom det også for teleselskap gjelder en kontraheringsplikt. Oppstillingen er også egnet for å vise mulighetsrommet for kostnadspulverisering som foreligger for kontotilbyder. Både bruk av konto og kontoeierskap kan gebyrbelegges av kontotilbyder. For kontotilbyder vil også tjenestetilbudet begrense seg til rent faktisk egne kundeforhold, i motsetning til teleselskap hvor kontraheringsplikten også gjelder levering av tjenester til andres kunder.

Innføringen av en informasjonsdelingsplikt fra fullmaktforetak til kontotilbyder vil også ha positive rettsøkonomiske virkninger. Et fullmaktforetak hjemmehørende i en stat som leverer fullmakttjenester til en kontoeier hjemmehørende i en annen stat med kundeforhold hos en kontotilbyder hjemmehørende i en tredje stat, vil sende MT-meldinger til FIU i sin hjemstat som deretter etter eget skjønn, oversetter og sender videre til kontoeiers hjemstat.

Det samme vil gjelde kontotilbyder uten stedlig representasjon i kontoeiers hjemstat. I så fall vil man kunne ende i en situasjon hvor FIU i tre stater vet litt hver, og ingen har hele bildet, før eventuelt de to respektive FIU-ene i henholdsvis fullmaktforetakets hjemstat og kontotilbyders hjemstat oversetter og videresender MT-meldingene til FIU i kontoeiers hjemstat. Til dette må det imidlertid bemerkes at i tråd med tidligere drøftelser i oppgaven og den påfølgende konklusjonen, vil situasjoner hvor fullmaktforetak kan tilføre vital informasjon i en MT-melding om et mistenkelig forhold som kontotilbyder selv ikke er lovpålagt å avdekke i hevd av undersøkelsesplikten, trolig være begrenset til rent hypotetiske situasjoner.

Det vil likefullt være positive rettsøkonomiske virkninger av å få ansvarliggjort kontotilbyder som en felles koordinator av kundeinformasjon om egne kontokunder som grunnlag for MT-meldinger sendt til FIU. Og selv om man legger til grunn at det spillteoretiske problemet oppstilt i forrige kapittel vedvarer for kontotilbyders vedkommende, vil det totale antallet MT-meldinger fra samme forhold likevel reduseres fordi fullmaktforetakene ikke lenger selv vil rapportere. Dette er i seg selv et gode.

Utvider man denne skisserte informasjonsdelingsplikten til et trepartssamarbeid mellom fullmaktforetak, kontotilbyder, og betalingsmottaker, vil man kunne oppnå ytterligere synergier. En slik løsning vil imidlertid representere et betydelig mer radikalt skifte fra dagens regime, ettersom det vil bety å innføre en fast praksis for å utveksle informasjon om kundeforhold med foretak uten kundeforhold til samme person. Informasjonsdeling etter dagens regler i AMLD4 kan kun skje

mellom to personer involvert i samme forhold for samme kunde.[148] Videre vil dette representere klare personvernmessige utfordringer og forutsette en betydelig teknologisk harmonisering for å kunne helautomatisere informasjonsdelingen.[149]

Et slikt trepartssamarbeid vil også i praksis måtte inkludere personer i tredjeland, for eksempel i det tilfellet hvor en kontoeier initierer en betaling fra en europeisk konto til en konto i et tredjeland. På andre rettsområder har man sett at avtale som hjemmel med aktører utenfor EU ofte ikke gir tilstrekkelig sikkerhet for etterlevelse, slik også Schrems II-dommen om overføring av personopplysninger til land utenfor EØS-området.[150]

Det synes likevel klart at fordelene med en EU-rettslig informasjonsdelingsplikt som skissert her, synes tilstrekkelig tungtveiende til at forslaget fortjener en nærmere vurdering, enten man begrenser det til kontotilbyder og fullmaktforetaket, eller også inkluderer betalingsmottakers kontotilbyder.

[148] AMLD4, artikkel 39 (5)
[149] Se ISO 20022
[150] C-311/18

8 Litteraturliste

8.1 EU-relevante rettskilder

8.1.1 Direktiver, forordninger, og avgjørelser

C-191/17. Dom av 31. desember, 2018 [C5]. Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG.

C-311/18. Schrems II. Dom av 16. juli, 2020 [GC]. Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems.

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive 2015/2366/EU 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.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

8.1.2 Forarbeid, rapporter, etterarbeid og uttalelser

AFEPAME. (u.å.). *Submission #23*. European Banking Authority. Besøkt 1. mai, 2021. Tilgjengelig på https://www.eba.europa.eu/node/99760/submission/95617

Financial Data and Technology Association Europe. (u.å). *Submission #33.* European Banking Authority. Besøkt 1. mai, 2021. Tilgjengelig på https://www.eba.europa.eu/node/99760/submission/95635

EBA/GL/2021/02. Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849. (The ML/TF Risk Factors Guidelines).

EBA-OP-2016-07. Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD).

Ehrmann, Michael & Ampudia, Miguel. (2017). *"Financial inclusion: what's it worth?," Working Paper Series 1990, European Central Bank*. Besøkt 1. mai, 2021. Tilgjengelig på https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1990.en.pdf

European Commission. (2015). *European Parliament adopts European Commission proposal to create safer and more innovative European payments*. Besøkt 8. mai, 2021. Tilgjengelig på https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5792

European Police Office. (2016). *Does crime still pay? Criminal asset recovery in the EU – survey of statistical information 2010–2014.* Tilgjengelig på https://www.europol.europa.eu/publications-documents/does-crime-still-pay

European Police Office. (2017). *From suspicion to action - converting financial intelligence into greater operational impact.* Besøkt 2. mai, 2021. Tilgjengelig på https://www.europol.europa.eu/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf

European Banking Federation. (2017). *EBF asks Commission to support ban on screen scraping.* Besøkt 10. mars, 2021. Tilgjengelig på ebf.eu/wp-content/uploads/2017/05/EBF_027173-EBF-asks-EU-not-to-disregard-EBA-recommendation-on-PSD2.pdf

GREEN PAPER Towards an integrated European market for card, internet and mobile payments /* COM/2011/0941 final */

Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

8.2 Norske rettskilder

Bergen tingretts dom 20. februar, 2019 (TBERG-2018-51923).

Finanstilsynet. (2020). *Finanstilsynets virksomhetsregister*. Besøkt 10. mai, 2021. Tilgjengelig på https://www.finanstilsynet.no/virksomhetsregisteret/

Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven)

Lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)

Politidirektoratet & Politiets sikkerhetstjeneste. (2020). *Nasjonal risikovurdering – hvitvasking og terrorfinansiering 2020*. Besøkt 4. mars, 2021. Tilgjengelig på https://www.okokrim.no/ny-nasjonal-risikovurdering-om-hvitvasking-og-terrorfinansiering.6354385-411472.html

8.3 Litteratur

Arner, Douglas W., Janos Barberis og Ross P. Buckley. (2016). *The evolution of FinTech: A new post-crisis paradigm*. Georgetown Journal of International Law.

Akter, Sajeda, Chellappan, Sriram, Chakraborty, Tusher, Khan, Taslim Arefin, Rahman, Ashikur, & Alim Al Islam, Abm. (2020). *Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection.* IEEE Transactions on Dependable and Secure Computing, 1. https://doi.org/10.1109/tdsc.2020.3030213

Dhar, Payal. (2020). *The carbon impact of artificial intelligence.* Nature Machine Intelligence, 2(8), 423–425. https://doi.org/10.1038/s42256-020-0219-9

Lammerts, I., Ma, D., Ploeger, N., Deutekom, B. A., van Eerten, S. J., Vink, N., Wagemakers, T. N., Sanders, K. I. M., Visser, C. L. S., & Schaap, R. B. (2017). *The second European payment services*

directive (PSD2) and the risks of fraud and money laundering. AMLC. Besøkt 20. mars, 2021. Tilgjengelig på: https://www.amlc.eu/wp-content/uploads/2019/04/The-PSD2-and-the-Risks-of-Fraud-and-Money-Laundering.pdf

Nicoletti, Bernardo. (2017). *The Future of FinTech.* Springer Publishing.

Ornaghi, A., & Valleri, M. (2003). *Man in the middle attacks.* Blackhat Conference Europe (Vol. 1045).

Grohé, Susanne. (2018). *AML, Payment Initiation Services & Account Information Services.* PayTechLaw.Com. Besøkt 30. mars, 2021. Tilgjengelig på https://paytechlaw.com/en/the-devil-is-in-the-detail-should-payment-initiation-services-and-account-information-services-be-subject-to-aml-regulations/

Romānova, I., Grima, S., Spiteri, J., & Kudinska, M. (2018). *The Payment Services Directive 2 and competitiveness: the perspective of European Fintech companies.* European Research Studies Journal, 21(2), 5-24.

Rui, Jon Petter. (2012). *Hvitvasking: Fenomenet, regelverket, nye strategier*. Universitetsforlaget. ISBN 978-8-2150-2054-9.

Saltkjel, Janne Britt. (2019). *PSD2 – transformasjon eller disrupsjon?* Praktisk Økonomi & Finans, 35(02), 98–109. https://doi.org/10.18261/issn.1504-2871-2019-02-03

Savona, Ernesto Ugo & Riccardi, Michele (Eds.). (2015). *From illegal markets to legitimate businesses: the portfolio of organised crime in Europe.* Final Report of Project OCP – Organised Crime Portfolio. Trento: Transcrime – Università degli Studi di Trento.

Skoghøy, Jens. Edvin A. (2018). *Rett og rettsanvendelse*. Universitetsforlaget. ISBN 978-8-2150-2858-3.

Takáts, Elod. (2011). *A Theory of "Crying Wolf" : The Economics of Money Laundering Enforcement*. Journal of Law, Economics, and Organization, 27(1), 32-78. https://doi.org/10.1093/jleo/ewp018

8.4 Personlig kommunikasjon, foredrag, og intervju

Beyrouthy, Elie. (2021). Styreleder for European Payment Institutions Federation. Personlig meddelelse om PSD2 og AMLD4, 4. mai, 2021.

Furset, Daniel Isdal. (2021). Driftssjef i Fintech Norway. Personlig meddelelse om PSD2, 4. mai, 2021.

Grimstad, Erling. (2019). *Hvitvasking – fra sorte til hvite penger*. Paneldebatt på Arendalsuka 13. september, 2019. Sitert 13. mars, 2021. Tilgjengelig på https://youtu.be/Yo6T396yvfI

Olsen, Odd Atle. Senior IT Architect i DNB. Personlig meddelelse om betalingsoverføringer, 21. mai, 2021.

Strømsnes, Kristian. (2021). Postdoktor Ph.D ved Universitetet i Bergen. Personlig meddelelse om grønbøkers EU-rettslige vekt, 8. april, 2021.

Rhysider, Jack. (2021). Ep 85: Cam the carder. Darknet Diaries. Besøkt 1. mai, 2021. Tilgjengelig på https://darknetdiaries.com/episode/85/

8.5 Avisartikler, nyhetsartikler og debattinnlegg

Eroglu, Hakan. (2018). *Berlin Group and the path to PSD3*. FinExtra. Besøkt 8. mai, 2021. Tilgjengelig på https://www.finextra.com/blogposting/16389/berlin-group-and-the-path-to-psd3

Hopland, Sindre. (2019). *Får bedriftskonto for bitcoin-handel etter nesten seks år kamp mot bankene*. E24.no. Besøkt 1. mai, 2021. Tilgjengelig på https://e24.no/naeringsliv/i/Jo7916/faar-bedriftskonto-for-bitcoin-handel-etter-nesten-seks-aar-kamp-mot-bankene

Jain, Shubham. (2020). *Identifying and Preventing Money Laundering in a Pandemic*. Corporate Compliance Insights. Besøkt 20. februar, 2021. Tilgjengelig på https://www.corporatecomplianceinsights.com/preventing-money-laundering-in-pandemic/

Rui, Jon Petter & Søreide, Tina. (2020). *Tiltakene mot hvitvasking koster mer enn de smaker.* Dagens Næringsliv. Besøkt 1. mai, 2021. Tilgjengelig på https://www.dn.no/innlegg/hvitvasking/korrupsjon/okokrim/innlegg-tiltakene-mot-hvitvasking-koster-mer-enn-de-smaker/2-1-767790 [Kronikk]

Schultz, Jacob. (2019). *De tre største bankene i Norge har brukt over 15 milliarder kroner på å bekjempe økonomisk kriminalitet. Dagens Næringsliv*. Besøkt 1. mai, 2021. Tilgjengelig på https://www.dn.no/marked/thomas-midteide/hans-thrane-nielsen/jan-petter-sissener/de-tre-storste-bankene-i-norge-har-brukt-over-15-milliarder-kroner-pa-a-bekjempe-okonomisk-kriminalitet/2-1-7186180

8.6 Elektroniske utgivelser

Asen, Elke. (2021). *Corporate income tax rates in Europe.* Tax Foundation. Besøkt 3. mars, 2021. Tilgjengelig på https://taxfoundation.org/2020-corporate-tax-rates-in-europe/

Basel Institute on Governance. (2020). *Public Ranking.* Besøkt 10. april, 2021. Tilgjengelig på https://baselgovernance.org/basel-aml-index/public-ranking

Bundesanstalt für Finanzdienstleistungsaufsicht. (u.å.). *BaFin - Zahlungsinstituts- und E-Geld-Instituts-Register nach §§ 43, 44 ZAG. Bafin.De.* Besøkt 22. april, 2021. Tilgjengelig på https://portal.mvp.bafin.de/database/ZahlInstInfo/

De Best, Raynor. (2020). *Payment methods in Europe - statistics & facts.* Statista. Besøkt 20. mars, 2021. Tilgjengelig på https://www.statista.com/topics/3946/digital-payment-methods-in-europe/

Federal Financial Institutions Examination Council. (u.å.). *FFIEC BSA/AML*. Besøkt 15. april, 2021. Tilgjengelig på https://bsaaml.ffiec.gov/error/405/

Hernæs, Christoffer. (2019). *The definitive guide to open banking*. Hernaes.com. Besøkt 15. april. Tilgjengelig på https://hernaes.com/2019/08/07/the-definitive-guide-to-open-banking/

ISO 20022. Besøkt 19. mai, 2021. Tilgjengelig på https://www.iso20022.org/

Johnsen, Brynjel. (2019). *PSD2 – Status på oppløpssiden.* Besøkt 5. mars, 2021. Tilgjengelig på https://static1.squarespace.com/static/562a32b0e4b0e6f4ec3104ae/t/5c8b6faf652dea8792d1cb27/1552641976261/BRYNJEL+JOHNSEN+-+PSD2+%E2%80%93+Status+p%C3%A5+oppl%C3%B8pssiden.pdf

KPMG. (2019). *Malta's tax system.* KPMG.com.mt. Besøkt 14. april, 2021. Tilgjengelig på https://assets.kpmg/content/dam/kpmg/mt/pdf/2019/12/malta-tax-system.pdf

LexisNexis Risk Solutions. (2017). *The true cost of anti-money laundering compliance.* Besøkt 22. april, 2021. Tilgjengelig på https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey

Mathias, Richard. (2019). *How ecommerce merchants can prepare for PSD2*. Econsultancy.com. Besøkt 30. mars, 2021. Tilgjengelig på https://econsultancy.com/ecommerce-merchants-prepare-psd2/

MerchantSavvy.co.uk. (2020). *50+ Global Mobile Payment Stats, Data & Trends (Feb 2020)*. Besøkt 12. mars, 2021. Tilgjengelig på https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/

Pedersen, Rune. (2021). *Oversikt over rabatter og andre fordeler du får i kredittkortene*. Besøkt 26. mai, 2021. Tilgjengelig på https://www.smartepenger.no/markedsoversikter/846-fordeler-du-far-i-kredittkortene

Stenseth, Børre. (2014). *iframe*. Besøkt 10. mai, 2021. Tilgjengelig på https://borres.hiof.no/wep/htm/iframe/index.html

United Nations Office on Drugs and Crime. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes.* Besøkt 29. februar, 2021. Tilgjengelig på https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Xero. (u.å.). *Xero Central*. Xero. Besøkt 8. mai, 2021. Tilgjengelig på https://central.xero.com/s/article/Xero-Releases#2011

Yapily.com. (2020). *PSD2: What you need to know about Screen Scraping and API's.* Besøkt 20. februar, 2021. Tilgjengelig på https://www.yapily.com/blog/psd2-screenscraping-apis/

9 Liste over figurer

Figur 1, s. 10: Bolton, Natasja. (2020). *Payment Services Directive (EU) 2015/2366 (PSD2) & Strong Customer Authentication.* Sysnet Global Solutions. Hentet 6. juni, 2021. Tilgjengelig på https://sysnetgs.com/2019/01/eu-payment-services-directive-2017-psd2-strong-customer-authentication/

Figur 2, s. 11: Bolton, Natasja. (2020). *Payment Services Directive (EU) 2015/2366 (PSD2) & Strong Customer Authentication.* Sysnet Global Solutions. Hentet 6. juni, 2021. Tilgjengelig på https://sysnetgs.com/2019/01/eu-payment-services-directive-2017-psd2-strong-customer-authentication/

Figur 3, s. 21: Imperva.com. (u.å.). *What is MITM (Man in the Middle) Attack*. Hentet 6. juni, 2021. Tilgjengelig på https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/