UiO : Det juridiske fakultet

Overvåking av betalingstransaksjoner

En sammenlignende analyse av plikter til å avdekke og undersøke ikke godkjente betalingstransaksjoner og hvitvaskingstransaksjoner

Kandidatnummer: 204

Leveringsfrist: 10. november

Antall ord: 39 392

Innholdsfortegnelse

Del I: Innledning, sentrale hensyn og rettslige utgangspunkter

1 Innledning

1.1 Tema og problemstillinger

Finansnæringen er en av de mest digitale næringene i Norge.[1] Løsninger for nettbank og mobilbank gir tilgang til enkle og trygge banktjenester for mange. BankID, som er en løsning for elektronisk identifikasjon («eID»), har muliggjort digitalisering av banktjenester. Løsningen har også fått vid utbredelse til andre formål i privat og offentlig sektor. De siste årene har det imidlertid vært en økning i profesjonelle svindlere som retter målrettede angrep mot norske bankkunder.[2] Metodene er sofistikerte, og selv digitalt oppegående kunder har problemer med å gjennomskue svindlerne.[3]

Det er ofte organiserte kriminelle miljøer med internasjonale tilknytninger som står bak storskalasvindlene.[4] Det at kriminelle opparbeider seg økonomiske midler som følge av bedragerier har ifølge Økokrims økt så voldsomt og nådd et slikt omfang at det er et nasjonalt sikkerhetsproblem.[5]

Hvitvasking og terrorfinansiering er følgeutfordringer av den kriminelle virksomheten. Bedrageriene er primærlovbrudd[6] som skaper utbytte som den kriminelle deretter forsøker å hvitvaske og/eller bruke til terrorfinansiering eller annen alvorlig kriminalitet. Hvitvasking er i straffeloven definert som befatning med utbytte fra straffbare handlinger,[7] hvor formålet er å finne en metode for å føre illegale midler og verdier inn i finanssystemet.[8] Egenskapen til hvitvasking er at den skjuler pengestrømmen, slik at det fra utsiden ser ut som om pengene stammer fra legitime handlinger. Misbruk av betalingssystemet er en velkjent metode for hvitvasking.

Betalingssystemet er i utgangspunktet avhengig av tillit.[9] Viktige aktører på området som Økokrim,[10] Kripos,[11] Finanstilsynet[12] og Skatteetaten[13] fremholder at kriminell utnyttelse av betalingssystemet i form av bedragerier og hvitvasking av bedrageriutbyttet utfordrer tilliten og

[1] Meld. St. 18 (2022–2023) Finansmarkedsmeldingen 2023, s. 48.
[2] DNB/FCR (2022) s. 2.
[3] DNB/FCR (2022) s. 7.
[4] Finanstilsynet (2023) s. 11; Europol (2021) s. 19.
[5] Økokrim (2023a) s. 31.
[6] Lov 20. mai 2005 nr. 29 om straff (straffeloven – strl.) § 371.
[7] Strl. §§ 332 og 337.
[8] NOU 2016: 27 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering andre delutredning, s. 27 fl.
[9] Norges Bank (2022) s. 11.
[10] Økokrim (2023a) s. 6, 14, 16; Økokrim (2023b) s. 31.
[11] Politiet/Kripos (2023) s. 24–25.
[12] Finanstilsynet (2023) s. 7.
[13] Skatteetaten (2021) s. 11.

sikkerheten i samfunnet. For å sikre tilliten til banktjenester er foretakene derfor avhengige av å håndtere risikoen for svindel og hvitvasking.

Bruken av overvåkingsmekanismer er anerkjent som et av de viktigste tiltakene for å håndtere risikoene for svindel og hvitvasking.[14] På den bakgrunn vil jeg i denne avhandlingen gjøre en rettsdogmatisk og rettspolitisk analyse av utvalgte overvåknings- og undersøkelsesforpliktelsene som følger av *forskrift om systemer for betalingstjenester,*[15] *finansavtaleloven*,[16] *hvitvaskingsloven*,[17] og *hvitvaskingsforskriften.*[18]

Forskrift om systemer for betalingstjenester § 12 fastsetter plikt til å anvende transaksjonsovervåkningsmekanismer for å avdekke ikke godkjente betalingstransaksjoner. Finansavtaleloven oppstiller undersøkelsesplikter på bakgrunn av tilbakeføringsplikten i fil. § 4-32 og tapsfordelingsregler i fil. § 4-30. Etter hvitvaskingsloven følger overvåknings- og undersøkelsesforpliktelsene av foretakets plikt til å følge opp kunden, jf. hvvl. § 24, iverksette nærmere undersøkelser, jf. hvvl. § 25, og rapportere mistanke om hvitvasking eller terrorfinansiering til Økokrim, jf. hvvl. § 26. Videre oppstiller hvitvaskingsforskriften § 7-3 minstekrav til elektroniske overvåkningssystemer.

Formålet med pliktene etter forskrift om systemer for betalingstjenester og finansavtaleloven er å sikre at transaksjoner ikke gjennomføres uten at de er godkjent av kunden. Det reiser spørsmål om balanseringen mellom hensynet til effektivitet i betalingsformidlingen mot hensynet til beskyttelse av kunden mot risikoen for å bli utsatt for svindel.[19] Formålet med pliktene etter hvitvaskingsloven og hvitvaskingsforskriften er å forhindre og avdekke befatning med kriminelt utbytte, for å beskytte det finansielle systemet og samfunnet som helhet mot hvitvasking og terrorfinansiering.[20]

Formålene etter de to regelsettene er ikke sammenfallende. Som analysen i det følgende vil avdekke innebærer imidlertid forpliktelsene etter begge regelsett at foretaket skal avdekke unormal kundeaktivitet. Paradokset betalingsinstitusjonen står overfor i gjennomføringen av en betalingstransaksjon er at banken på den ene siden skal beskytte kunden mot misbruk og bedra-

[14] COM(2023) 367 final, avsnitt 100; FATF (2014) avsnitt 73.

[15] Forskrift om systemer for betalingstjenester 15. februar 2019 nr. 152.

[16] Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven – fil.).

[17] Lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven – hvvl.).

[18] Forskrift om tiltak mot hvitvasking og terrorfinansiering 14. september 2019 nr. 1324 (hvitvaskingsforskriften).

[19] For nærmere redegjørelse om formålene, se punkt 4.2 og 8.2.

[20] For nærmere redegjørelse om formålene, se punkt 5.2 og 9.2.

geri, og på den andre siden avdekke kriminelle kunder for å beskytte finanssystemet og samfunnet for øvrig mot skadevirkningene av hvitvasking. Unormal kundeaktivitet kan enten tilsi at kunden er i ferd med å *utsettes* for noe kriminelt, eller at kunden *er* kriminell.

Til tross for stor oppmerksomhet omkring risikoene for svindel og hvitvasking hver for seg, er forholdet mellom forpliktelsene etter nevnte regelverk i liten grad vært utforsket. For betalingsforetak er det av betydning å vite hvordan rutiner og systemer skal utformes for å sikre etterlevelse. Det er behov for en nærmere analyse av overvåkings- og undersøkelsespliktene, hvor siktemålet er å få en mer helhetlig forståelse av sikkerhetskravene som stilles og deres betydning for gjennomføring av betalingstransaksjoner. Dette ønsker jeg å gjøre med denne avhandlingen.

En analyse av overvåkings- og undersøkelsesplikten favner en rekke større og mindre problemstillinger som får betydning for hverandre. Av den grunn har jeg funnet det mest hensiktsmessig å foreta en helhetlig analyse, hvor de overordnede problemstillingene er:

> *Hva innebærer overvåkings- og undersøkelsespliktene? Er pliktene egnet til å oppfylle sine formål? Og hvordan forholder pliktene etter de to regelsettene seg til hverandre?*

For å besvare problemstillingene vil jeg for det første fastlegge innholdet i overvåkings- og undersøkelsespliktene. For å forstå pliktenes innhold og rekkevidde er det nødvendig å redegjøre for den samfunnsmessige konteksten som lå til grunn for pliktenes vedtakelse, samt begrunnelsen for at lovgiver så behov for plikter til å overvåke betalingstransaksjoner. Et sentralt poeng er at betalingstjenesteyter skal forhindre økonomisk kriminalitet, og skal ikke medvirke til eller tjene på at det utøves kriminelle handlinger. Betalingstjenesteyter må på den bakgrunn sørge for sikkerhet i betalingsformidlingen og utføre nødvendige kontroller i den forbindelse.

For det andre vil jeg undersøke om pliktene er egnet til å oppfylle sine respektive formål. Vurderingen av måloppnåelse vil bygge på den rettsdogmatiske undersøkelsen. Jeg vil gjøre en rettspolitisk vurdering av pliktenes klarhet og tilgjengelighet, samt diskutere effektiviteten av de økonomiske insentivene til å etterleve forpliktelsene. Hensikten er å belyse mulige svakheter i regelverket som kan hindre at formålet med pliktene blir realisert i praksis.

Til sist vil jeg undersøke hvordan pliktene forholder seg til hverandre. Etterlevelse av begge regelsett nødvendiggjør bruk av automatiserte overvåkingssystemer. Alarmer i transaksjonsovervåkingen kan få betydning både for svindeltransaksjoner og hvitvaskingstransaksjoner. I den sammenlignende analysen er det derfor det interessant å analysere pliktenes anvendelsesområde og rekkevidde fordi formålene etter de to regelsettene ikke er sammenfallende. I den forbindelse

vil jeg undersøke noen av de grensedragningene foretaket står ovenfor i overholdelse av pliktene som tar sikte på å beskytte kunden mot svindel, og pliktene som tar sikte på å beskytte det finansielle systemet og samfunnet mot hvitvasking og terrorfinansiering. Målet er å belyse mulig motstrid mellom enkelte av pliktene, og fremheve potensielle utfordringer når foretakene involvert i gjennomføringen av en betalingstransaksjon skal etterleve begge regelverk.

I analysen av de ovennevnte pliktene avgrenser jeg til overvåking av fjernbetalingstransaksjoner.[21] Dette er en type elektronisk betalingstransaksjon hvor det er avstand mellom betaler og betalingsmottaker, som eksempelvis internetthandel eller andre transaksjoner ut av nettbank, til forskjell fra bruk av betalingskort i butikk.[22] EU har identifisert at denne typen betalingstransaksjoner er mest utsatt for svindel, og derfor har størst behov for implementeringen av sikkerhetstiltak.[23]

1.2 Rettskildebildet

1.2.1 Overvåkings- og undersøkelsespliktenes EØS-rettslige bakgrunn – gjennomføringen i norsk rett

Rettskildebildet er relativt omfattende og komplekst. I det følgende vil jeg derfor introdusere de viktigste rettskildene og deres EØS-rettslige bakgrunn.

Det reviderte betalingstjenestedirektivet («PSD 2») ble vedtatt i 2015 og utgjør den overordnede rammen for betalingsformidlingen i EU og EØS.[24] PSD 2 oppstiller rettslige rammer for ytelsen av betalingstjenester, og skal sikre vern av kundens rettigheter, og balansere kundebeskyttelse opp mot hensynet til effektivitet i finansmarkedet.[25] Den Europeiske Kommisjonen har i 2023 forslått endringer av PSD 2,[26] samt foreslått en ny forordning.[27]

---

[21] Europaparlaments- og rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (PSD 2), artikkel 4 (6).

[22] For nærmere begrepsavklaring, se punkt 1.4.

[23] PSD 2, fortalen avsnitt 95.

[24] PSD 2 fortalen avsnitt 2.

[25] PSD 2 fortalen, avsnitt 6; Europaparlamentets- og rådets direktiv 2007/64/EC af 13. november 2007om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF (PSD I), fortalen avsnitt 4.

[26] COM(2023) 367 final.

[27] COM(2023) 366 final.

Av PSD 2 følger regler for initiering og gjennomføring av betalingstransaksjoner. Pliktene av offentligrettslig preg er gjennomført i norsk rett ved endring i betalingssystemloven og finansforetaksloven,[28] og resulterte blant annet i endringen av forskrift om systemer for betalingstjenester § 5 som gjennomfører kravet til sterk kundeautentisering ved initiering av elektroniske betalingstransaksjoner.[29] I tillegg til innføringen av kravet til sterk kundeautentisering følger det av direktivet at betalingstjenesteytere må være autorisert av nasjonale myndigheter og registreres av det europeiske banktilsynet, The European Banking Authority («EBA»).[30] Videre må bankene åpne opp sine Application Programming Interfaces («API») overfor tredjeparter. API-er er et grensesnitt som tillater at ulike systemer snakker med hverandre og deler informasjon.[31]

I tillegg til vedtagelsen av PSD 2 ble *delegert kommisjonsforordning*[32] («RTS») vedtatt i 2018, som er en regulatorisk teknisk standard utarbeidet av EBA på bakgrunn av PSD 2 artikkel 98 (1)(a). PSD 2 artikkel 98 gir EBA myndighet til å spesifisere vilkårene for sterk kundeautentisering som referert til i PSD 2 artikkel 97 (1) og (2). RTS er vedtatt som forordning i EU, og er inkorporert i norsk rett i forskrift om systemer for betalingssystemer § 12.[33] Endringen trådte i kraft 25. juli 2023. Forordningen gjelder som norsk forskrift med de tilpasninger som følger av EØS-avtalen vedlegg IX, og regulerer tekniske sikkerhetskrav til *anvendelsen* av sterk kundeautentisering. Deriblant følger krav til overvåking av ikke godkjente betalingstransaksjoner.[34]

De privatrettslige delene av direktivet er gjennomført i *finansavtaleloven*.[35] Finansavtaleloven kapittel 4 regulerer betalingstjenesteyterens plikter til gjennomføring av betalingstransaksjoner,[36] samt plikter overfor kunden ved gjennomføring av ikke godkjente betalingstransaksjoner.

---

[28] Loven ble endret ved lov nr. 87/2018.

[29] PSD 2 artikkel 97.

[30] Se listen her: EUCLID - Register (europa.eu).

[31] Ofoeda, Boateng og Effah (2019) s. 76–77.

[32] Delegert kommisjonsforordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation (RTS).

[33] Forskriften ble endret ved forskrift nr. 1245.

[34] RTS artikkel 2.

[35] Prop.92 LS (2019–2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014, s. 18.

[36] Fil. § 4-6.

Når det gjelder antihvitvaskingsreguleringene fra EU er *det fjerde hvitvaskingsdirektivet*[37] fra 2015 det viktigste juridiske dokumentet. Direktivet er et rammeverk for å håndtere kriminalitetsbekjempelse ved å kreve at medlemsstatene identifiserer, forstår og reduserer risikoene knyttet til hvitvasking av penger og finansiering av terrorisme.[38] Den viktigste endringen i det fjerde hvitvaskingsdirektivet fra det tredje hvitvaskingsdirektivet er at pliktene legger opp til risikobaserte tiltak mot hvitvasking og terrorfinansiering, til forskjell fra en regelbasert tilnærming.[39] Bakgrunnen for den risikobaserte tilnærmingen i direktivet er de reviderte anbefalingene til den finansielle aksjonsgruppen, The Financial Task Force («FATF»), fra 2012.[40]
I Norge gjennomfører *hvitvaskingsloven* tiltakene i det fjerde hvitvaskingsdirektivet.[41]

Videre har EU i 2018 vedtatt det femte hvitvaskingsdirektivet,[42] som reviderer enkelte bestemmelser i det fjerde hvitvaskingsdirektivet. EØS-komiteen vedtok i 2020 å innlemme EUs femte hvitvaskingsdirektiv i EØS-avtalen.[43] I tillegg står det sjette hvitvaskingsdirektivet[44] på trappene, som er ment å erstatte det fjerde hvitvaskingsdirektivet.

For å presisere det nærmere innholdet i og omfanget av pliktene etter hvitvaskingsloven har Finansdepartementet fastsatt *hvitvaskingsforskriften,* som blant annet presiserer minstekrav til anvendelsen av elektroniske overvåkingssystemer.[45] Hvitvaskingsforskriften gjennomfører i hovedsak revisjonene i det femte hvitvaskingsdirektivet. Som del av Finanstilsynets forvaltning av hvitvaskingsloven har tilsynet videre utarbeidet *rundskriv til hvitvaskingsloven*.[46] Rundskrivet gir blant annet veiledning om hvordan foretaket skal gjennomføre kundetiltak og nærmere undersøkelser, og hva som skal til for å rapportere til Økokrim.

---

[37] Europaparlamentets- og rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (det fjerde hvitvaskingsdirektivet – 4AMLD).

[38] 4AMLD, fortalen avsnitt 3.

[39] 4AMLD, fortalen avsnitt 22;

[40] 4AMLD, fortalen avsnitt 3.

[41] NOU 2016:27 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering andre delutredning, s. 15.

[42] Europaparlamentets rådsdirektiv (EU) 2018/843 af 30. maj 2018 om ændring af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme og om ændring af direktiv 2009/138/EF og 2013/36/EU (det femte hvitvaskingsdirektivet – 5AMLD).

[43] Se regjeringens EØS-notatbase 14. februar 2020 (https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2016/nov/forslag-til-endring-av-eus-fjerde-hvitvaskingsdirektiv/id2525237/).

[44] COM/2021/423 final.

[45] Hvitvaskingsforskriften § 7-3.

[46] Veileder til hvitvaskingsloven 15. november 2022 (RFT-2022-4).

1.2.2 Arbeider fra EBA – uttalelser og retningslinjer

I tillegg til PSD 2 sine krav til initiering av betalingstransaksjoner, og pliktene i det fjerde hvitvaskingsdirektivets til risikobaserte tiltak mot hvitvasking og terrorfinansiering, har EBA publisert en rekke uttalelser og retningslinjer.[47] Myndigheten til å utforme uttalelser og retningslinjer følger av EBAs opprettelsesforordning artikkel 16.[48] Formålet med uttalelsene og retningslinjene er å sikre en felles, ensartet og konsekvent anvendelse av EU-retten,[49] og er følgelig sentrale virkemidler for å sikre uniform forvaltningspraksis på EU-rettens område.[50]

Uttalelser og retningslinjer fra EBA er ikke formelt bindende.[51] Det følger imidlertid av Finanstilsynets uttalelser at den tar EBAs uttalelser og retningslinjer i betraktning, og forventer at også pliktsubjektene til de underliggende EØS-rettslige forpliktelsene tar uttalelsene og retningslinjene i betraktning.[52] I praksis er dermed uttalelsene og retningslinjene relevante rettskilder som norske betalingstjenesteytere må forholde seg til.

1.2.3 FATFs anbefalinger

I tillegg til at hvitvaskingsloven gjennomfører det fjerde hvitvaskingsdirektivet, er loven ment å følge opp evalueringsrapporten til Financial Task Force (FATF) fra 2012 om norsk etterlevelse av det felleseuropeiske hvitvaskingsreglementet.[53] FATF ansees som en premissleverandør for det internasjonale arbeidet for å bekjempe hvitvasking og terrorfinansiering.[54] FATF er en samarbeidsgruppe med 39 medlemsland, herunder Norge, som gjennomfører landevalueringer og produserer detaljerte rapporter av landets etterlevelse av utarbeidede standarder. Den siste evalueringen av Norge ble publisert februar 2023.[55]

---

[47] Avhandlingen vil vise til følgende uttalelser og retningslinjer fra EBA: EBA/Op/2017/09; EBA-Op-2018-04; EBA-Op-2019-06; EBA/Op/2022/06; EBA/GL/2022/15; EBA/Op/2023/08.

[48] Europarlamentets- og rådets direktiv (EU) Nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (opprettelsesforordningen).

[49] Opprettelselsforordningen artikkel 16 (1).

[50] Hertzberg og Bekkedal (2018) s. 205–226.

[51] Opprettelsesforordningen artikkel 16 (3).

[52] Se følgende nyhetsmeldinger fra Finanstilsynet; 21. juni 2019 om EBAs uttalelse om sterk kundeautentisering under PSD 2 (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2019/sterk-kundeautentisering-under-psd2/); 22. april 2022 om EBAs uttalelse om unntak fra sterk kundeautentisering (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2022/unntak-fra-sterk-kundeautentisering/); 23. juni 2023 om EBAs retningslinjer om kundeetablering uten personlig fremmøte (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2023/retningslinjer-fra-eba-om-kundeetablering-utan-personleg-oppmote-trer-i-kraft-2.-oktober-2023); 9. august 2023 om EBAs uttalelse om hvitvaskingsrisiko (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2023/uttale-fra-eba-om-risikoen-for-kvitvasking-og-terrorfinansiering/).

[53] NOU 2016: 27 s. 15.

[54] Meld. St. 18 (2022–2023) s. 57.

[55] FATF (2023).

Sett hen til at både EU-kommisjonen og en rekke EU-land er medlem av FATF, påvirker FATF EU sitt arbeid i utviklingen av hvitvaskingsdirektivet. I fortalen til det fjerde hvitvaskingsdirektivet uttales at forpliktelsene i direktivet skal være i samsvar med, og minst like strenge som FATFs anbefalinger.[56] FATF sine standarder er følgelig relevante for tolkningen av direktivet. Der standarden gjennomføres i EUs rettsakter og disse tas inn i EØS-avtalen, blir standarden bindende for Norge. I den grad anbefalingene ikke er gjennomført via direktivforpliktelsen, er de hensyntatt i utformingen av hvitvaskingsloven.[57]

1.2.4 Forvaltningspraksis

Finanstilsynet har en viktig rolle ved håndhevelsen av overvåkingsforpliktelsene i Norge. Finanstilsynet har ansvar for å føre tilsyn med etterlevelsen av forskrift om systemer for betalingstjenester.[58] Det følger av forskrift om systemer for betalingssystemer § 2 at foretaket minst årlig skal gi Finanstilsynet en samlet vurdering av operasjonell risiko og sikkerhetsrisiko knyttet til tilbyderens betalingstjenester, samt om tilbyderens tiltak er tilstrekkelige. I tillegg skal betalingstjenestetilbydere minst årlig rapportere statistikk om svindel knyttet til betalingstjenestene på den måten Finanstilsynet angir.[59]

Finanstilsynet har også ansvar for tilsynet av brorparten av de rapporteringspliktiges overholdelse av pliktene i hvitvaskingsloven,[60] blant annet banker, kredittforetak og betalingsforetak. Overtredelse av hvitvaskingsloven er straffesanksjonert, jf. hvvl. § 51, og kan videre sanksjoneres med overtredelsesgebyr etter hvvl. § 49.[61]

For pliktene som følger av finansavtaleloven har også forbrukertilsynet en viktig rolle. Forbrukertilsynet fører tilsyn med at næringsdrivendes avtalevilkår og handelspraksis som rettes til forbrukere ikke er i strid med ufravikelig forbrukerlovgivning, på grunnlag av forbudet mot urimelig handelspraksis i markedsføringsloven § 6.[62] Dette innebærer at Forbrukertilsynet kan føre indirekte tilsyn med overholdelsen av ufravikelige forbrukervernregler.[63] Fra 1. januar 2023 fører Forbrukertilsynet direkte tilsyn med at reglene i ny finansavtalelov overholdes overfor forbrukere.[64]

---

[56] 4AMLD, fortalen avsnitt 4.

[57] NOU 2016: 27 s. 14; Prop. 40 L (2017–2018) Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven), s. 10.

[58] Forskrift om systemer for betalingstjenester § 2.

[59] Gjennomfører RTS artikkel 21.

[60] Hvitvaskingsloven § 43 (2)(a).

[61] Departementet valgte ikke å innføre særskilte hjemler for administrativt rettighetstap i hvitvaskingsloven, se begrunnelsen i Prop.40 L (2017–2018), punkt 10.7.3.3.

[62] Lov av 9. januar 2009 nr. 2 om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven).

[63] Fil. § 3-55.

[64] Se forbrukertilsynets nettsider https://www.forbrukertilsynet.no/nye-reglar-styrkar-forbrukarvernet.

Forvaltningspraksisen utgjør et viktig grunnlag for avhandlingens rettspolitiske betraktninger av om pliktene er egnet til å oppfylle sine formål.

1.3 Metode

1.3.1 Den rettsdogmatiske analysen

I avhandlingen skal jeg bruke rettsdogmatisk metode for å fastlegge innholdet av utvalgte regler om overvåkings- og undersøkelsesplikter i det finansregulatoriske regelverket. En utfordring i analyser av finansregulatoriske regelverk er den rettskildemessige kompleksiteten og fraværet av rettspraksis. I tillegg forgår forvaltningspraksisen fra Finanstilsynet og Forbrukertilsynet i stor grad i dialog med foretakene.[65] På den bakgrunn vil et særlig fokus i avhandlingen være å systematisere pliktene.

Reglene jeg skal fastlegge innholdet av, gjennomfører EØS-rettslige forpliktelser. Det innebærer at de norske reglene må tolkes i overenstemmelse med de krav rettsaktene oppstiller, i tråd med prinsippet om direktivkonform tolkning. Kort sagt innebærer prinsippet at nasjonale regler skal tolkes i samsvar med folkerettslige forpliktelser etter EØS-avtalen.[66] I *Finanger I* ga Høyesterett sin tilslutning til prinsippet, og slo fast at prinsippet om EU-konform ikke går lenger enn presumpsjonsprinsippet i norsk rett.[67] Det følger av presumpsjonsprinsippet at norske bestemmelser så vidt mulig skal gis et innhold som samsvarer med Norges folkerettslige forpliktelser.[68]

PSD 2 stiller krav til fullharmonisering.[69] Det betyr at medlemsstatene ikke kan beholde eller innføre regler som fraviker reglene i direktivet. De norske reglene må derfor tolkes slik at de ikke pålegger betalingstjenesteytere strengere forpliktelser enn det som følger av direktivet.

Det fjerde hvitvaskingsdirektivet er til sammenligning et minimumsdirektiv.[70] Det betyr at medlemsstatene har adgang til å fastsette strengere regler enn det som følger av direktivet. De norske reglene må tolkes slik at de ikke gir dårligere vern enn det som følger av direktivet.

---

[65] Se eksempelvis tilsynsrapport 21/395.

[66] Se eksempelvis Rt. 2001 s. 1006 s. 1015 og Rt. 2010 s. 1445 avsnitt 133.

[67] Rt. 2000 s. 1811.

[68] I etterkant av Finanger I har det skjedd en rettsutvikling i EU-domstolen angående tolkning av EU-rett, se eksempelvis C-371/02 *Björnekulla* og C-441/14 *Ajos*, som kan antyde at prinsippene om EU-konform tolkning rekker lenger enn presumsjonsprinsippet i norsk rett. I rammene av denne avhandlinger ser jeg det ikke som nødvendig å gå nærmere inn på dette.

[69] PSD 2 artikkel 107.

[70] 4AMLD artikkel 4 (1) og artikkel 5.

Ved tolkningen av internasjonale forpliktelser skal de internasjonale normene for tolkning som gjelder for den konkrete forpliktelsen følges. Ved tolkning av direktivene må derfor den EØS-rettslige metode anvendes. Jeg legger til grunn at EØS-rettslig metode i hovedsak er lik som EU-rettslig metode. Jeg vil i korte trekk peke på noen føringer i EU-rettslig metode med betydning for denne avhandlingen.

I EU-retten byr ordlydstolkning på noen utfordringer, da reglene er utformet på flere språk, og språkversjonene er likestilte. Ordlydstolkningen nødvendiggjør derfor sammenligning av ordlyden i de ulike språkdraktene.[71] Jeg har valgt i hovedsak å vise til den danske språkdrakten, og har gjennomgående sammenlignet med den svenske og engelske ordlyden. Der det er relevant viser jeg også til disse språkversjonene. Når det gjelder RTS er forordningen oversatt til norsk, men den norske versjonen er ikke ennå kunngjort.[72] Jeg vil av den grunn vise til den danske språkdrakten, også når det gjelder forordningen.

På bakgrunn av utfordringene tilknyttet ordlydstolkningen står en systemorientert og formålsrettet tolkning av EU-retten særlig sterkt for tolkningen. En formålsrett tolkning sikrer blant annet uniform etterlevelse av reglene i medlemsstatene. Formålene med overvåkings- og undersøkelsespliktene skal jeg se nærmere på i punkt 4.2, 5.2, 8.2, og 9.2.

Et metodisk spørsmål for den videre analysen er den rettskildemessige relevansen til EBAs uttalelser og retningslinjer. Den rettskildemessige statusen til EBAs arbeider for norsk rett med EØS-rettslig forankring er ikke helt klargjort.[73] På tross av at uttalelsene og retningslinjene ikke er formelt bindende, kan uttalelser fra EU-domstolen allikevel tas til inntekt for at de er relevante kilder for fastleggelse den innholdsmessige normen som følger av den aktuelle EU-rettslige normen. Eksempelvis uttaler EU-domstolen i sak C-322/88 *Grimaldi* på avsnitt 18 at nasjonale rettsinstanser skal ta hensyn til fellesskapsrettslige kilder selv om de ikke er direkte bindende, når disse «kan bidrage til fortolkningen af nationale bestemmelser udstedt til gennemfoerelse heraf, eller naar der er tale om henstillinger, som har til formaal at udfylde bindende faellesskabsretlige bestemmelser». Det trekker i retning av at i den grad uttalelsene og retningslinjene om PSD 2 og det fjerde hvitvaskingsdirektivet kan gi veiledning om innholdet i den nasjonale forpliktelsen er de ikke bindende arbeidene til EBA relevante tolkningsmomenter.

[71] Neergaard og Nielsen (2021) s. 113.

[72] EØS-tillegget til Den europeiske unions tidende Nr. 34/61 (2023/EØS/34/17).

[73] Hertzberg og Bekkedal (2018) s. 205-226.

Tolkningen underbygges av at Finanstilsynet har lagt til grunn at norske foretak tar arbeidene fra EBA i betraktning.[74] Uttalelsene fra Finanstilsynet kan forstås som uttrykk for forvaltningens rettsoppfatning. Av den grunn vil arbeidene til EBA bli vektlagt i den videre analysen av overvåkings- og undersøkelsespliktene.

Norske rettskilder som uttaler seg om tolkningen av direktivbestemmelsene, som uttalelser i forarbeidene eller uttalelser fra Finanstilsynet, har til sammenligning mer begrenset vekt. Det betyr ikke at nasjonale rettskilder er uten betydning. Ofte er løsningen åpen eller uklar fra et EU-perspektiv. I den grad EØS-rettslige kilder ikke løser spørsmålet vil jeg ta hensyn til norske kilder. I fastleggelsen av kravene vil dermed forarbeidene til finansavtaleloven og hvitvaskingsloven og forvaltningspraksis få betydning. Rundskriv og veiledere fra forvaltningen vil i tråd med Høyesteretts rettskildebruk anvendes i avhandlingen som støtteargument for slutninger med rettskildemessig grunnlag i de andre rettskildefaktorene.[75]

1.3.2 Den rettspolitiske vurderingen

På bakgrunn av den rettsdogmatiske analysen av overvåkings- og undersøkelsespliktenes innhold og rekkevidde vil jeg foreta en vurdering av om pliktene er egnet til å oppfylle sine formål.[76] I vurderingen av regeleffektiviteten vil jeg komme med rettspolitiske betraktninger der jeg mener det kan være behov for endring. De rettspolitiske betraktningene er oppfatninger om hvordan retten *bør* være, i motsetning til en rettsdogmatisk analyse som sier hva gjelder rett *er*.

I den rettspolitiske vurderingen vil jeg for det første se på pliktenes klarhet og tilgjengelighet. Dersom en plikt har et uklart innhold eller uklar rekkevidde kan det lede til mangelfull etterlevelse. I den forbindelse er det et spørsmål om pliktene kommer til anvendelse overfor de identifiserte relevante problemene. Vurderingen vil bygge på kartleggingen av problemet med digitale bedragerier og hvitvasking i avhandlingens kapittel 2.

For det andre vil jeg undersøke foretakenes insentiv til å etterleve forpliktelsene. Økonomiske insentiver er et anerkjent tiltak for å oppmuntre til etterlevelse.[77] Økonomiske insentiver kan oppnås gjennom risiko for å bli ilagt offentligrettslige sanksjoner og straff, samt gjennom regulering av privatrettslig tapsrisiko.[78] Effektiviteten av offentligrettslige sanksjoner og straff vil kunne avhenge av hvor intensivt foretakene underlegges offentlig kontroll og tilsyn. Den pri-

[74] Se https://www.finanstilsynet.no/regelverk/eba-retningslinjer/eba-retningslinjer/.

[75] Se eksempelvis Rt. 2013 s. 1601.

[76] Se nærmere om formålene i punkt 4.2, 5.2, 8.2, og 9.2.

[77] Sheedy, Zhang, Tam (2019); Stulz (2015) s. 8-18.

[78] Se eksempelvis uttalelser fra departementet i Prop.92 LS (2019–2020) på s. 184 fl.

vatrettslige tapsrisikoen kan avhenge av tilgangen på rettssystemet, og muligheten for å påberope mislighold. Videre kan det tenkes vekselvirkning mellom offentligrettslige sanksjoner og privatrettslig tapsrisiko, der brudd på offentligrettslige plikter kan ansees erstatningsbetingende uaktsomt. For å vurdere effektiviteten til insentivene vil jeg undersøke etterlevelsen av forpliktelsene ved å gjennomgå forvaltningspraksis og relevant rettspraksis.

I vurderingen av regeleffektivitet er det andre momenter som kan ha betydning for om formålene med en plikt blir oppfylt i praksis. Til illustrasjon kan *muligheten* til å oppfylle forpliktelsen ha betydning, eksempelvis dersom de tekniske løsningene på markedet er mangelfulle. Denne typen vurderinger faller imidlertid utenfor denne avhandlingen.

1.4 Avgrensninger og begrepsavklaringer

Avhandlingen omhandler overvåkingsforpliktelser som gjelder for betalingstjenesteytere, som i fil. § 1-5 (9) er legaldefinert som «en tjenesteyter som tilbyr finansielle tjenester som er omfattet av kapittel 4». Ordlyden peker på kapittel 4 til finansavtaleloven, som gjelder retten til kontoavtale og betalingstjenester. Avhandlingen vil fokusere på betalingstjenester. Med betalingstjenester menes i finansavtaleloven en tjeneste med meldeplikt eller krav om særskilt tillatelse etter finansforetaksloven, jf. fil. § 1-5 (5), og som omfatter en av de opplistede aktivitetene i fil. § 1-5 (1) bokstav a til h.[79] I tråd med avhandlingens forskningsspørsmål vil jeg fokusere på gjennomføring av betalingstransaksjoner, jf. § 1-5 (1) bokstav c og d. Det følger av listen i bokstav c og d at det omfatter direkte debiteringer, bruk av betalingskort, instruks om kontobetaling og kreditoverføringer.[80]

Avhandlingen avgrenser videre til å vurdere pliktene relevant for gjennomføringen av fjernbetalingstransaksjoner. Fjernbetalingstransaksjoner er i PSD 2 artikkel 4 (6) definert som «en betalingstransaktion, der initieres via internettet eller gennem en anordning, der kan anvendes til fjernkommunikation». Definisjonen er presisert i fortalen til PSD 2, som i avsnitt 95 omtaler denne typen transaksjoner som «[b]etalingstjenester, der udbydes på internettet eller via andre fjernkanaler, og hvis funktion ikke afhænger af, hvor den anordning, der anvendes til at initiere betalingstransaktionen, eller det anvendte betalingsinstrument er fysisk placeret». Det følger av det ovenstående at en betalingstransaksjon er fjern der den initieres via internett eller, i tilfelle transaksjonen initieres via en enhet, der enhetens fysiske tilstedeværelse er irrelevant for initieringen av betalingstransaksjonen.[81] Med mindre noe annet er presisert vil begrepene betalingstransaksjon og fjernbetalingstransaksjon i det følgende benyttes som synonymer.

[79] Gjennomfører PSD 2 artikkel 4 (3), jf. vedlegg I.

[80] Fil. § 1-5 (1)(c) og (d).

[81] EBA-2019-4594; EBA-2020-5367; EBA-2020-5247.

Etter finansforetaksloven § 2-3 er det kun «banker, kredittforetak, betalingsforetak, e-pengeforetak og opplysningsfullmektiger og av finansieringsforetak» med tillatelse etter finansforetaksloven som har rett til å yte betalingstjenester, herunder gjennomføre betalingstransaksjoner. I avhandlingen vil jeg benytte begrepet «betalingstjenesteyter» for å omtale de nevnte finansforetakene i finansforetaksloven § 2-3, i tråd med finansavtalelovens begrepsbruk. For variasjonens skyld vil jeg også benytte begrepet «foretak» og «betalingsforetak».

Pliktene som følger av RTS har, i tråd med PSD 2, betalingstjenesteytere som pliktsubjekter. Hvitvaskingsloven derimot pålegger en rekke juridiske og fysiske personer plikter til å forebygge og avdekke hvitvasking, jf. angivelsen av rapporteringspliktige i hvvl. § 4 (1), (2) og (5), jf. § 2 bokstav c. Hvitvaskingsloven har følgelig et langt videre nedslagsfelt enn avhandlingen tar sikte på å behandle. I tråd med avhandlingens forskningsspørsmål avgrenser jeg til å behandle pliktene som er relevante for betalingstjenesteytere. Ethvert finansforetak med rett til å yte betalingstjenester er pliktsubjekt i henhold til hvitvaskingsloven, jf. hvvl. § 4 (1) bokstav g. Når jeg i avhandlingen behandler pliktene etter hvitvaskingsloven vil jeg omtale betalingstjenesteytere som «rapporteringspliktige» i tråd med hvitvaskingslovens begrepsbruk.

Formålet til hvitvaskingsloven er overordnet «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. hvvl. § 1 (1). I analysen av pliktene etter hvitvaskingsloven med forskrift vil jeg i hovedsak fokusere på bekjempelse av hvitvasking. Hvitvasking er definert i hvitvaskingsloven som «handling som beskrevet i straffeloven § 332 og 337», jf. hvvl. § 2 bokstav a. Hvitvasking slik det er definert i loven omfatter følgelig også det som etter norsk rett omtales som heleri. Det innebærer at hvitvasking omfatter all befatning med verdier som stammer fra straffbare handlinger.[82]

Definisjonen av hvitvasking viser at loven er ment å komme til anvendelse overfor en rekke handlinger. Der finanssystemet misbrukes til å hvitvaske penger vil imidlertid transaksjonen eller aktiviteten normalt involvere et finansforetak.[83] En transaksjon er definert i hvitvaskingsloven som «enhver overføring, formidling, ombytting eller plassering av formuesgoder», jf. hvvl. § 2 bokstav d. I tråd med avhandlingens forskningsspørsmål avgrenser jeg til pliktene som er relevante for gjennomføring av direkte debiteringer, bruk av betalingskort, instruks om kontobetaling og kreditoverføringer, jf. fil. § 1-5 (1) bokstav c og d, der initieringen er en fjernbetalingstransaksjon.

[82] NOU 2016: 27 s. 219.
[83] NOU 2016: 27 s. 34.

1.5 Avhandlingens videre fremstilling

For å sette avhandlingen inn i en kontekst og begrunne aktualiteten til problemstillingene som vil bli behandlet, beskrives problemet med digitale bedragerier og hvitvasking i kapittel 2. I tillegg presenteres de generelle reglene for initiering av betalingstransaksjoner som den videre fremstillingen vil bygge på.

Avhandlingens hoveddel følger av del II og III hvor jeg vil se nærmere på kravene som stilles til utforming av rutiner og systemer for overvåking, og betydningen av alarmer i overvåkingen for foretakenes undersøkelsesplikt. I tråd med avhandlingens forskningsspørsmål innebærer det å fastlegge pliktenes nærmere innhold, om pliktene er egnet til å oppfylle sine formål, samt forholdet mellom pliktene. I avhandlingens avsluttende del vil jeg samle trådene, og oppsummere avhandlingens mest sentrale funn.

2 Bakgrunn, rettslige utgangspunkter og sentrale hensyn

2.1 Problemet med digitale bedragerier

I Finanstilsynets risiko- og sårbarhetsanalyse («ROS») fra 2023 er cyberkriminalitet fremhevet som den største risikoen mot den finansielle infrastrukturen.[84] Organisert cyberkriminalitet som informasjonsinnhenting, salg av informasjon om digitale sårbarheter, phishing-kampanjer[85] og penetrering av finansforetakenes digitale beskyttelsesmekanismer er nevnt som de mest fremtredende trusselfaktorene.[86] Som ledd i organisert cyberkriminalitet rapporterer Finanstilsynet i ROS særlig om økt kriminell aktivitet knyttet til nettsvindel.[87] Til illustrasjon undersøkte DNB 6 550 phishingangrep i 2022. [88] Det er en økning med 69 prosent i 2022 fra 2021, og en 920 prosent økning sammenlignet med 2020.

Som Kripos fremhever i temarapporten om cyberkriminalitet fra 2023 er svindel knyttet til BankID og sosial manipulasjon, samt at privatpersoner utsettes for ID-tyveri med påfølgende bedragerier, viktige årsaker til økningen og utbredelsen av digitale bedragerier.[89] DNB sin svindelavdeling peker videre på at kvaliteten på angrepene øker.[90] Det innebærer at også normalt forsiktige personer blir lurt. Denne utviklingstrenden gjenfinnes ikke bare i Norge. Det at kriminelle nettverk utøver mer kriminalitet i det digitale rom eller benytter digitale løsninger i

[84] Finanstilsynet (2023) s. 11 fl.

[85] «Phishing» er et angrep der angriperen bruker sosial manipulering for å utføre identitetstyveri. Phishing fungerer tradisjonelt ved å sende forfalsket e-post som etterligner en nettbank, auksjons- eller betalingssider, og lede brukere til en falsk nettside som er nøye utformet for å se ut som påloggingen til det ekte nettstedet, jf. Aleroud, Zhou (2017) s. 160-196.

[86] Finanstilsynet (2023) s. 11.

[87] Finanstilsynet (2023) s. 11 og 30 fl.

[88] DNB/FCR (2022) s. 3; Se også tilsvarende tendens i EU, jf. Europeiske sentralbanken (2018) s. 7.

[89] Politiet/Kripos (2023) s. 35–36; Skatteetaten (2021) s. 4, 13.

[90] DNB/FCR (2022) s. 7.

gjennomføringen av og samhandlingen med sikte på kriminaliteten, er en tendens i hele Europa.[91]

Som illustrert i straffesaken behandlet av Høyesterett i HR-2022-2468-A kan digitale bedragerier få store konsekvenser. I saken for Høyesterett lå de fullbyrdede bedrageriene på til sammen 17,8 millioner kroner.[92] Ifølge Økokrim er det ikke uvanlig at det enkelte offer taper flere hundre tusen kroner, og i noen tilfeller millionbeløp, særlig i tilfelle av investeringsbedrageri og kjærlighetsbedrageri.[93]

Det at bedrageriene lykkes med å generere store summer til kriminelle får ringvirkninger med potensielle skadevirkninger for tilliten til digitale banktjenester og til digitale tjenester mer generelt.[94] En tendens avdekket av Økokrim, som synliggjør hvordan tilliten og sikkerheten i samfunnet blir skadelidende, er at de kriminelle reinvesterer utbyttet fra bedrageriene i annen kriminell virksomhet.[95] Dette er en tendens som kan gjenfinnes i andre europeiske land. Eksempelvis i Sverige er det avdekket at bedragerier finansierer grov voldskriminalitet.[96] I Storbritannia er det avdekket at bedrageriene har gått til å finansiere terrorisme, som blant annet IS.[97] I tillegg inngår bedrageri som cyberkriminalitet i et større globalt sikkerhetsproblem knyttet til risiko og sårbarheter i den digitale infrastrukturen.[98] I ROS-rapporten fra 2023 fremhever Finanstilsynet risikoen for cyberangrep fra andre stater, illustrert ved Russlands cyberangrep mot Ukraina lenge før krigen ble igangsatt,[99] og digitale angrep brukt som politisk virkemiddel, som tjenestenektangrepet mot BankID sommeren 2022 er et eksempel på.[100]

For å skjule sin tilknytning til utbytte fra bedrageri ser Økokrim utstrakt bruk av såkalte pengemuldyr. [101] Bruken av pengemuldyr er en velkjent metode for å hvitvaske utbytte fra kriminelle handlinger. Ifølge Økokrim er pengemyldyrene i mange tilfeller også ofrene for bedrageriet.[102] I tillegg har Økokrim registrert en økende tendens i å rekruttere unge sårbare personer. Det er

---

[91] Europol (2021) s. 19.

[92] HR-2022-2468-A avsnitt 16 og 25.

[93] Økokrim (2023a) s. 5.

[94] Se også uttalelser av Høyesterett i HR-2022-2468 avsnitt 20.

[95] Økokrim (2023a) s. 5; Europol (2021) s. 19.

[96] Polismyndigheten (2022) s. 21.

[97] Wood, Keatinge, Ditcham og Janjeva (2021) s. 29 fl.

[98] Finanstilsynet (2023) punkt 3.3 og 3.4; Økokrim (2023a) s. 7.

[99] Brombach, «Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap», *Digi.no*, 24. februar 2022.

[100] Svigghum et. al., «BankID og Arbeidstilsynets nettsider er nede - ustabilitet i Altinn», *e24*, 29. juni 2022.

[101] Økokrim (2023a) s. 5.

[102] Økokrim (2023a) s. 13.

ifølge Økokrim snakk om ungdom ned i 13–14 års alderen som både stiller kontoen sin til disposisjon, tar uttak fra konto i kontanter, eller overfører penger videre.[103]

Siden både hvitvasking og digitale bedragerier utnytter sårbarheter i det digitale kontaktpunktet mellom kunde og bank er de to kriminelle handlingene nært knyttet sammen. Det nære forholdet mellom bedragerier og hvitvasking byr imidlertid på noen særlige utfordringer. I politietterforskningen av profittmotivert kriminalitet er en velkjent problematikk at politiet ofte har bevismessige vansker med å knytte såkalte bakmenn til konkrete primærlovbrudd.[104] Som beskrevet av hvitvaskingsutvalget i arbeidet med hvitvaskingsloven er en vanlig modus at bakmennene holder en slik distanse fra primærlovbruddet at det ikke er mulig eller svært vanskelig å knytte dem til kriminaliteten.[105] Utvalget peker på at bakmennene ofte er mer involvert i den etterfølgende befatningen med utbyttet fra lovbruddene.

Ved utstrakt bruk av pengemuldyr vil det imidlertid være pengemuldyrene og ikke bakmennene som deltar i den umiddelbare befatningen av utbyttet fra bedrageriene. Det oppstår en risiko for at politiet straffeforfølger pengemuldyrene og ikke bakmennene. De kriminelle kan utnytte identiteten til pengemuldyret til vedkommende blir straffeforfulgt, og identiteten er «brukt opp». Sett hen til at pengemuldyrene i bedragerisakene ofte enten er bedrageriofferet selv eller unge sårbare rekrutterte personer kan det indikere at tilgangen på identiteter er for enkel.

Det nære forholdet mellom bedragerier og hvitvasking byr også på utfordringer for betalingsforetaket. For foretaket er det for det første en utfordring knyttet til i det hele tatt å avdekke at betalingstransaksjonen har tilknytning til kriminalitet. For det andre er det en utfordring knyttet til å skille situasjonen der betalingstransaksjonen er resultat av et bedrageri mot kunden, fra situasjonen der kunden forespør gjennomføring av en betalingstransaksjon som ledd i hvitvasking av kriminelt utbytte. Sagt på en annen måte, når betalingsinstitusjonen avdekker en illegitim betalingstransaksjon kan kunden potensielt være et offer for kriminalitet eller selv være en kriminell.

2.2 Om svindel- og hvitvaskingsrisiko etter gjennomføringen av PSD 2 i norsk rett

I etterkant av vedtagelsen av det første betalingstjenestedirektivet fra EU i 2007 skjedde det en voldsom utvikling i det elektroniske betalingsmarkedet, særlig på bakgrunn av fremveksten av

[103] Økokrim (2023a) s. 5 og 13.
[104] NOU 2016: 27 s. 22.
[105] NOU 2016: 27 s. 22.

API-økonomien.[106] API-økonomien har vært en viktig bidragsyter til suksessen til store selskaper som Amazon, Google, Uber, med mer, ved å tilrettelegge for utviklingen av en ny forretningsmodell, som eksempelvis fintech-selskaper.

I forlengelsen av fremveksten av API-økonomier har fintech-selskaper gjort sitt inntog på betalingsmarkedet. Fintech er teknologi brukt til å forenkle ytelsen av finansielle tjenester og leveringen av tjenesten til kunder, eksempelvis gjennom å automatisere ulike prosesser. [107] Typiske eksempler er tilgang til nettbank via applikasjoner («mobile banking»), betalingstjenester som Vipps («peer-to-peer» betalingstjenester), samt utviklingen og handel med kryptovaluta. Fintech-selskapers virksomhet falt imidlertid ikke inn under anvendelsesområdet til det første betalingstjenestedirektivet.[108]

Som svar på teknologisk innovasjon i betalingssystemer kom PSD 2 på plass i 2015, primært for å imøtekomme et integrert europeisk marked for kort-, internett- og mobilbetalinger. Nærmere bestemt var det nødvendig å gjøre det mulig å gi tredjeparter tilgang på kontotilbyders API og hente ut betalers kontodata, for blant annet å igangsette betalinger på deres vegne direkte fra bankkontoen. PSD 2 sikrer økt utnyttelse av betalingstjenestene ved å legge opp til informasjonsdeling mellom betaler, kontotilbyder og betalingsmottaker i gjennomføringen av betalingstransaksjoner.[109]

De økte sikkerhetsrisikoene for svindel og hvitvasking etter vedtakelsen av PSD 2 er for det første *risikoen for upålitelige og kriminelle tredjeparter*. Tredjepartenes tilgang på kontohavers kontoinformasjon medfører risiko for at kontoinformasjonen blir misbrukt til å begå identitetskrenkelse, ulovlig prisdiskriminering, eller å bli solgt videre. Kriminelle som ønsker å begå identitetssvindel kan infisere eksisterende tredjeparter med skadelig programvare, samt sette opp tilsynelatende legitime tredjeparter for å tilrettelegge for falske betalinger, og/eller for å få tilgang på en stor mengde med personsensitiv informasjon.

Kunden kan komme i kontakt med uredelige tredjeparter ved å skrive inn personlige opplysninger på falske nettsider eller mobilbetalingsapplikasjoner. Et sikkerhetsproblem i denne forbindelse er kundens manglende mulighet til å vurdere påliteligheten til tredjeparten og den betalingsinfrastrukturen som blir tilbudt. Kunden er i utgangspunktet ikke i en posisjon til å for-

[106] API-økonomien refererer til settet med forretningsmodeller og praksis designet rundt bruken av applikasjonsprogrammeringsgrensesnitt (API) i dagens digitale økonomi, jf. SWIFT (2017), s. 5–6.

[107] Puschmann (2017) s. 69–76.

[108] Romanova (2018) s. 3-22.

[109] I neste punkt vil jeg se nærmere på reglene i PSD 2 for informasjonsdelingen.

handle om autentiseringsprosedyrer, og har ikke forutsetninger for å vurdere betalingsinfrastrukturen som blir tilbudt. Dette er ikke nye risikoer. Tilretteleggingen i PSD for økt tilgang på kontoinformasjon kan imidlertid tilføre nye utfordringer.

For det andre er det økt sikkerhetsrisiko tilknyttet *misbruk og phishing av data*. Banker har i en årrekke advart mot ikke å oppgi sine konfidensielle innloggingsopplysninger til utenforstående.[110] Samtidig innebærer PSD 2 at kunder kan gi tredjeparter tilgang til kontoinformasjon ved å avgi «samtykke».[111] Hvordan kundens samtykke blir avgitt vil avhenge av bankens API.[112] Banken kan eksempelvis tillate at tredjeparten overfører betalingstjenestebrukerens legitimasjon til banken, eller banken kan velge å kreve at tredjeparten re-dirigerer kunden til bankens domene.[113]

Det kan være forvirrende for den enkelte kunde å avgjøre om henvendelsen om å avgi sikkerhetsinformasjon er legitim eller illegitim. En forsterkende faktor er at det for kunden kan være uklart hva vedkommende faktisk samtykker til, og hva konsekvensene av samtykke innebærer. Det aksentuerer risikoen for at kriminelle bygger nettsteder eller betalingapper som presenterer seg som en legitim innloggingsside eller betalingsside, og introduserer falske skjermer som tilsynelatende er identiske med autentifikasjonsgrensesnittet til kontotilbyder eller tredjeparten for å få tilgang til konfidensiell data.

Behovet for å beskytte kunden mot seg selv kan også oppstå der kundens sikkerhetsopplysninger kommer på avveie gjennom svindlers misbruk av relasjonen med kunden. I nære relasjoner kan svindler utnytte tillitsforhold og behov for hjelp til å bruke digitale løsninger.[114] Et eksempel på dette er der kunden gir opplysninger til en nærstående for det formål å få hjelp til bruk av BankID, og sikkerhetsopplysningene deretter blir misbrukt eller kommer på avveie til å gjennomføre ytterligere transaksjoner.[115] Et annet eksempel er svindel i nære relasjoner, hvor den ene parten skaffer seg tilgang på partners eller familiemedlemmers sikkerhetsopplysninger for å ta opp lån og gjennomføre transaksjoner av låneutbyttet.[116] Svindler kan også bruke mer inngripende metoder, som utpressing, tvang og vold. Det er grunn til å tro at misbruk av sikkerhetsopplysninger i nære relasjoner er en måte å utøve partnervold på.[117]

---

[110] Se eksempelvis uttalelser i FinKN-2023-31; Sml. standardvilkårene for utstedelse av BankID punkt 4, jf. Bits (2019) Avtalevilkår for PersonBankID og AnsattBankID – PDS.

[111] Nærmere om kravet til «samtykke» i neste punkt.

[112] RTS artikkel 30 (3).

[113] EBA-2021-6245.

[114] NorSIS (2023).

[115] Se til illustrasjon FinKN-2018-305 og FinKN-2021-36.

[116] Se til illustrasjon TSOFT-2017-175325 (Oslo tingrett), hvor en sønn misbrukte begge sine foreldres BankID til å ta opp lån for å finansiere egen spillavhengighet.

[117] Foley (2003) s. 21-22.

Svindelmetoden som gjerne kalles «kjærlighetssvindel», samt svindelmetoden som kalles «direktørbedrageri» har noen likehetstrekk med de ovennevnte metodene, idet det er offerets tillit som blir utnyttet.[118] Forskjellen fra ovennevnte svindelmetoder er at kunden blir manipulert til selv å foreta betalingen. Denne typen svindel omtales gjerne under paraplybetegnelsen autorisert betalingssvindel.[119]

En tredje sikkerhetsrisiko knytter seg til *kriminalitetsoppdagelse*. PSD 2 er, i tråd med direktivets målsetning,[120] ventet å innebære en økning i internasjonal handel. Det gjør det enklere å skjule penger i utlandet. Tredjeparter som initierer betalinger kan bistå kriminelle, enten om det er med vilje eller fordi de selv blir utnyttet av kriminelle. Aktørene ansvarlig for å forhindre og avdekke hvitvasking vil videre være spredt på forskjellige parter, og over potensielt flere landegrenser. Det kan gjøre det vanskeligere å avdekke og forhindre illegale pengestrømmer.

2.3 Rettslige utgangspunkter og sentrale hensyn

2.3.1 Initiering av betalingstransaksjoner

Som gjennomgangen av problemet med digitale bedragerier og hvitvasking i det foregående illustrerer, har betalingssystemet fått og vil fortsette å ha en betydelig rolle som sted for å utøve kriminalitet. Identiteter brukes og misbrukes for å gjennomføre bedragerier, og utbyttet blir deretter hvitvasket. For å undersøke grensedragningene mellom betalingsforetakets handleplikter til å avdekke og forhindre henholdsvis bedrageri og hvitvasking, må først de rettslige utgangspunktene klarlegges. Avhandlingens overordnede problemstilling gjelder plikten til å overvåke betalingstransaksjoner. Derfor skal jeg klarlegge hva en betalingstransaksjon er, hva som skal til for å initiere gjennomføringen av betalingstransaksjoner, og hvordan en betalingstransaksjon gjennomføres.

En «betalingstransaksjon» er i finansavtaleloven § 1-5 (6) definert som «en handling som iverksettes av betaleren eller på dennes vegne eller av betalingsmottakeren for å innbetale, overføre eller ta ut betalingsmidler, uten hensyn til eventuelle underliggende forpliktelser mellom betaleren og betalingsmottakeren».[121] Betaleren eller betalingsmottakeren iverksetter en betalingstransaksjon gjennom et «betalingsoppdrag», som etter finansavtaleloven § 1-5 (5) innebærer «en anmodning fra en betaler eller betalingsmottaker til en betalingstjenesteyter om å foreta en betalingstransaksjon».[122]

[118] DNB/FCR (2022) s. 5 og 6.
[119] Se eksempelvis LB-2022-74994.
[120] PSD 2, fortalen avsnitt 4.
[121] Gjennomfører PSD2 artikkel 4(5).
[122] Gjennomfører PSD2 artikkel 4(13).

En slik betalingsordre gis som oftest ved bruk av et «betalingsinstrument». Betalingsinstrument er i finansavtaleloven § 1-5 (2) definert som «en personlig innretning eller et sett av fremgangsmåter avtalt med betalingstjenesteyter som kan benyttes for å iverksette betalingsoppdrag». Eksempler på betalingsinstrument er bankkort, giroblanketter, og koder som gir tilgang til elektroniske betalingssystemer, som eksempelvis BankID. Som stadfestet av Høyesterett er BankID et betalingsinstrument når løsningen blir benyttet til å iverksette betalingstransaksjoner.[123]

Det følger av fil. § 4-2 (1) at «[e]n betalingstransaksjon anses som godkjent bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres». Kravet til «samtykke» som oppstilles i finansavtaleloven § 4-2 gir uttrykk for den grunnleggende forutsetningen at en transaksjon må godkjennes av kunden for at foretaket kan gjennomføre en betalingstransaksjon.

Det følger av finansavtaleloven § 4-2 (2) at samtykke til å gjennomføre en betalingstransaksjon eller en serie med betalingstransaksjoner «skal gis i den formen og på den måten som er avtalt mellom betaleren og betalingstjenesteyteren». Det følger av dette at prosedyren for å avgi samtykke, og herunder stegene betalingstjenesteyter bør ta for å sjekke om transaksjonen er autorisert, avhenger av hva som er avtalt mellom betalingstjenestebrukeren og dennes betalingstjenesteyter.[124] Der betaleren har fått utstedt en BankID vil den, i henhold til avtalen om utstedelse av BankID, kunne benyttes som sikkerhetsanordning ved betalingstransaksjoner.[125] Avtalen om utstedelse av BankID gir følgelig innehaveren mulighet til å foreta fremtidige betalingstransaksjoner. Det innebærer at når sikkerhetsanordningen til BankID brukes til å iverksette betalingstransaksjoner, avgis samtykke til at betalingstransaksjonen gjennomføres.

I tillegg følger det av forskrift om systemer for betalingstjenester at betalingstjenestetilbyderen må benytte «sterk kundeautentisering» i tre angitte situasjoner, jf. § 5 (1). En av disse tre situasjonene er gjennomføringen av elektroniske betalingstransaksjoner. Jeg vil av den grunn si noe mer om hva som menes med «autentisering» og «sterk kundeautentisering».

Det heter i fil. § 1-8 (8) at «autentisering» er en «fremgangsmåte som gjør det mulig for en betalingstjenesteyter å kontrollere identiteten til en kunde eller gyldigheten av et bestemt betalingsinstrument, herunder bruken av kundens personlige sikkerhetsinformasjon». Med «sterk kundeautentisering» menes «autentisering som bygger på bruk av to eller flere elementer som er kategorisert som kunnskap (noe bare brukeren vet), besittelse (noe bare brukeren har) og

[123] HR-2020-2021-A avsnitt 38; HR-2022-1752-A avsnitt 29; Se også Kjørven, Høgberg, Woxholth (2021) s. 335–366.

[124] EBA-2018-4440.

[125] Se eksempelvis Bits (2019) Avtalevilkår for PersonBankID og AnsattBankID – PDS, punkt 2.

iboende egenskap (noe brukeren er), som er så frittstående i forhold til hverandre at brudd på ett kriterium ikke innebærer risiko for brudd på de andre, og som er utformet på en slik måte at autentiseringsopplysningenes fortrolighet er sikret», jf. finansavtaleloven § 1-8 (9).[126]

Det følger av sammenhengen at ved gjennomføring av elektroniske betalingstransaksjoner må identiteten til kunden og bruken av kundens personlige sikkerhetsinformasjon tilknyttet et bestemt betalingsinstrument sikres gjennom en fremgangsmåte som baserer seg på bruk av to eller flere uavhengige elementer. Sikkerhetskravet til sterk kundeautentisering beskytter kundedata, slår fast brukerens identitet og reduserer risikoen for svindel. Et eksempel på løsning for sterk kundeautentisering som brukes på det norske markedet er BankID,[127] som skal tilfredsstille kravene til sikkerhetsnivå «betydelig» og «høyt» etter selvdeklarasjonsforskriften[128] §§ 3 og 4.

Som det følger av ordlyden til finansavtaleloven § 4-2 (2) annet punktum kan samtykke til å gjennomføre en betalingstransaksjon «også gis via betalingsmottakeren eller en betalingsfullmektig». Det samme følger av finansavtaleloven § 1-5 (5), som presiserer at også en betalingsmottaker kan gjennomføre en betalingstransaksjon. Forutsetningen er at betalingsmottaker bruker en tredjepart med tilgang til kontotilbyders API for det formål å initiere betalingstransaksjoner. Denne typen tredjeparter er i PSD 2 kalt «betalingsinitieringstjenesteudbyder».[129] For at tredjeparten kan få tilgang til kontohavers konto må kontohaver autentisere overfor sin kontotilbyder at tredjeparten kan få slik tilgang.[130] Ordlyden «samtykke» i finansavtaleloven § 4-2 rommer altså også situasjonen der betaleren autentiserer at en tredjepart kan få tilgang til betalerens konto.

I praksis er det i hovedsak tre metoder for tredjeparten å gjennomføre autentifikasjonsprosedyren av kundens samtykke,[131] herunder re-dirigering, innebygde tilnærminger og frakoblede tilnærminger. Et eksempel på re-dirigering er der betaleren kjøper varer på internett. Etter å ha lagt inn varer i «handlekurven» på internett, og kunden fortsetter til kassen, vil kunden bli bedt om å velge betalingsmåte. Der betaleren velger å betale via nettbanken vil betaleren bli re-dirigert til bankens innloggingside for å godkjenne betalingen.[132] Ved innebygde tilnærminger vil bankens innloggingsside være integrert i betalingssiden, uten at betaleren blir re-dirigert til

[126] Gjennomfører PSD2 artikkel 4(30).

[127] Bits (2019) punkt 1.3.

[128] Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon 21. november 2019 nr. 1578 (selvdeklarasjonsforskriften); Selvdeklarasjonsforskriften definerer sikkerhetsnivåer og tilsynsregime for elektroniske identifikasjonsordninger (eID-ordninger), jf. selvdeklarasjonsforskriften § 1

[129] PSD2 artikkel 4 (18), jf. vedlegg I.

[130] RTS artikkel 30 (2)(a).

[131] EBA/2018/Op/4, avsnitt 48 fl.

[132] EBA-2021-6245.

bankens side. Etter betalingen er godkjent blir betaleren tatt tilbake til selgers nettside. Følgelig innebærer ikke tredjepartens tilgang til kundens konto at tredjeparten får tilgang på kundens midler.[133]

Redegjørelsen viser at betalingstjenesteleverandørene er gitt stor frihet til å arrangere autentiseringen slik de finner mest hensiktsmessig. Det viser at EU i utformingen av normen om sterk kundeautentisering har lagt vekt på på innovasjon og konkurranse om sikkerheten til betalingskontoen, hvor betalingstjenesteleverandørene har rett til å stole på autentiseringsprosessen til banken. Dette er for å fremme utnyttelse av det elektroniske betalingsmarkedet, og er dermed i hovedsak et utslag av markedshensyn.

Kravet til sterk kundeautentisering fremmer videre hensynet til kundene, idet risikoen for misbruk reduseres. I tillegg bidrar sikkerhetskravet til å sikre kundens tillit til betalingsformidlingen. Sikkerhetskravet har dermed også et markedsfremmende hensyn.

2.3.2 Gjennomføringen av betalingstransaksjoner

Det rettslige utgangspunktet for gjennomføring av betalingstransaksjoner følger av finansavtaleloven § 4-6.[134] Det følger av bestemmelsens første ledd at

> «Med mindre noe annet er særskilt bestemt, kan betalingstjenesteyteren ikke nekte å gjennomføre et godkjent betalingsoppdrag når alle vilkårene i betalerens kontoavtale er oppfylt».

Det følger av ordlyden at foretaket som et utgangspunkt skal gjennomføre godkjente betalingsoppdrag. Som nevnt over beskriver betalingsoppdrag handlingen som anmoder betalingstjenesteytere om å gjennomføre en betalingstransaksjon, jf. fil. § 1-5 (5). Det sondres følgelig mellom betalingsoppdrag og betalingstransaksjoner. Ut ifra sammenhengen i regelverket er det en forutsetning for at det gjennomføres godkjente betalingstransaksjoner at anmodningen om å gjennomføre transaksjonen (altså betalingsoppdraget) er godkjent, jf. fil. § 4-2, jf. § 4-6.

I forarbeidene til legaldefinisjonene i fil. § 1-5 uttales det om sondringen mellom betalingsoppdrag og betalingstransaksjoner at «[f]or å utføre et betalingsoppdrag må betalingstjenesteyteren med andre ord utføre det som hører under den aktuelle tjenesteyterens ansvar i forbindelse med gjennomføring av en betalingstransaksjon».[135] Plikten i fil. § 4-6 (1) til å gjennomføre en betalingstransaksjon på bakgrunn av et «godkjent betalingsoppdrag» er en av disse forpliktelsene.

---

[133] PSD 2 artikkel 66 (3)(a).

[134] Gjennomfører PSD 2 artikkel 79 (2).

[135] Prop.92 LS (2019–2020) s. 343.

Gjennomføringen av betalingstransaksjoner skjer ved at betalerens konto «belastes», jf. fil. § 4-5 (1). Det følger av rammeverket for gjennomføring av betalingstransaksjoner mellom betalingstjenesteytere at belastningen av konto i praksis er en avregning mellom bankenes fordringsbalanser, som forvaltes av Norwegian Interbank Clearing System (NICS)[136] og Bits.[137] Belastning av konto innebærer å nedskrive det disponible beløpet på betalerens konto, og kreditere betalingsmottakers konto.[138]

Det følger videre av fil. § 4-5 (1) at kundens konto først belastes etter betalingsoppdraget er «mottatt» betalingstjenesteyter, jf. fil. § 4-5 (1). Tidspunktet for mottakelsen av betalingsoppdraget er regulert i annet ledd. I normaltilfeller hvor betalingen skjer på en virkedag ansees et betalingsoppdrag som mottatt «på samme tidspunkt som det blir levert til eller registrert hos betalerens betalingstjenesteyter», jf. fil. § 4-5 (2). Etter at betalingsoppdraget er «levert til eller registrert» skal betalerens betalingstjenesteyter etter fil. § 4-11 «sørge for at beløpet godskrives betalingsmottakerens betalingstjenesteyter». Bestemmelsen angir utløpet av visse frister betalerens betalingstjenesteyter må holde seg innenfor.

Fristene avhenger av hva slags type transaksjon det dreier seg om, jf.§ 4-11 (2). For betalinger som gjøres opp i NICS presiserer rammeverket ytterligere bestemte tidsfrister for avregning.[139] Avregning av straksbetalinger gjøres opp etter egne regler, hvor godskrivingen av beløpet skjer umiddelbart, mens avregningen skjer i ettertid.[140]

Det følger av det overnevnte at plikten til å gjennomføre godkjente betalingsoppdrag har til formål å sikre effektivitet og forutsigbarhet i betalingssystemet, og skal gjøre at de ulike aktørene i markedet kan stole på at transaksjoner gjennomføres rettidig.[141] Plikten til å gjennomføre godkjente betalingsoppdrag sikrer at bankene kan ha tillit til avregningen og oppgjøret seg imellom. Foretaket skal også sikre at betalingsmottakere kan stole på at betalinger gjennomføres. Reglene om oppgjør fremmer således i hovedsak hensynet til et effektivt marked.

---

[136] NICS eies av bankene og er et system for å avregne fordringer og forpliktelser mellom bankene. NICS Operatørkontor er konsesjonshaver og operatør for NICS. Norges Bank fører tilsyn med NICS, jf. NOU 2017:13 Ny sentralbanklov. Organisering av Norges Bank og Statens pensjonsfond utland, s. 188.

[137] Bits er en bransjeorganisasjon som eies av bankene (Om Bits - Bits AS).

[138] Se oversikt over den finansielle infrastrukturen i Norge i NOU 2017: 13 på s. 187–188.

[139] Bits (2023a) Regler for avregning og oppgjør av transaksjoner som inngår i Norwegian Interbank Clearing System (NICS).

[140] Bits (2023b) Regler om straksbetalinger med sikkert oppgjør.

[141] Se nærmere beskrivelse av betalingsoppgjøret mellom bankene i NOU 2017: 13 punkt 12.2.

Dersom betalingstransaksjoner gjennomføres uten betalerens samtykke ansees transaksjonen ikke som godkjent, jf. ordlyden «[e]n betalingstransaksjon anses som godkjent bare dersom betaleren har gitt sitt samtykke til at betalingstransaksjonen gjennomføres» i fil. § 4-2. Tapsfordelingen av ikke godkjente betalingstransaksjoner reguleres av fil. § 4-30. Hovedregelen i fil. § 4-30 (1) er at betalingstjenesteyter har ansvar for kundens tap som følge av ikke godkjente betalingstransaksjoner. Etter fil. § 4-32 skal betalingstjenesteyter tilbakeføre kundens tap etter kundens reklamasjon. Det følger av dette at risikoen for at det gjennomføres ikke godkjente betalingstransaksjoner er lagt til betalingstjenesteyter. Det fremmer i hovedsak hensynet til kundene.

Betalingstjenesteyternes plikter overfor øvrige markedsaktører på en side og pliktene overfor egne kunder på den annen side, illustrerer at foretaket i gjennomføring av betalingstransaksjoner står i et potensielt spenningsforhold mellom ulike hensyn. Utslaget av spenningsforholdet vil følge av den nærmere analysen av overvåkingspliktenes innhold og rekkevidde.

Del II: Om overvåkingsforpliktelsene

3 Innledende om transaksjonsovervåking

Som den videre fremstillingen vil vise er betalingsforetakene pålagt plikter til å utforme systemer og rutiner for å overvåke, for det første, autentiseringsprosedyren ved initiering av betalingstransaksjoner, jf. forskrift om systemer for betalingstjenester § 5, og for det andre, avvikende kundeadferd, jf. hvitvaskingsloven §§ 24 og 25.

Praktisk sett innebærer systemer og rutiner for transaksjonsovervåking at visse transaksjoner og transaksjonsmønstrene blir 'flagget', enten det skjer ved manuell eller elektronisk overvåking. Hensikten med flaggingen er å gjøre betalingsforetaket oppmerksom på mistenkelige transaksjoner eller transaksjonsmønstre. Jeg skal i det følgende først se nærmere på pliktene som følger av forskrift om systemer for betalingstjenester (kapittel 4) før jeg går over til pliktene som følger av hvitvaskingsloven med forskrift (kapittel punkt 5). Gjennomgangen vil avdekke hvilke transaksjoner og transaksjonsmønstre betalingsforetak skal ha kjennskap til.

Analysen vil avdekke at de to regelsettene stiller ulike krav til hvilke transaksjoner og transaksjonsmønstre betalingsforetak skal avdekke. På den bakgrunn vil jeg i kapittel 6 vurdere hvordan pliktene etter de to regelsettene forholder seg til hverandre. Undersøkelsespliktene pålagt betalingsforetaket som følge av funn avdekket i overvåkingen vil jeg behandle i del III.

4 Transaksjonsovervåking etter forskrift om systemer for betalingstjenester

4.1 Innledende bemerkninger

Kravene til overvåking springer ut av kravet til å sikre sterk kundeautentisering, jf. forskrift om systemer for betalingstjenester § 5 (1). For det første innebærer kravet til sterk kundeautentisering at betalingsforetaket overvåker at sterk kundeautentisering er benyttet ved initiering av elektroniske betalingstransaksjoner. Videre følger det av forskriftens § 5 (2) at betalingsforetaket skal «anvende sterk kundeautentisering som kobler transaksjonen til et spesifikt beløp og en spesifikk betalingsmottaker». I forordningen er kravet i forskriftens § 5 (2) omtalt som et krav til «dynamisk tilknytning», jf. RTS artikkel 5. Forordningen spesifiserer krav til bruk av «sikkerhetsforanstaltninger», herunder overvåkningssystemer, for å sikre dynamisk tilknytning.

I tillegg stiller RTS artikkel 2 krav til at betalingsforetaket overvåker transaksjonen for å kunne «afsløre uautoriserte eller svigagtige betalingstraktioner». I den nye finansavtaleloven har lovgiver valgt å bruke begrepet «ikke godkjent» i stedet for «uautorisert», men meningsinnholdet er det samme.[142]

Kravet til overvåking i RTS artikkel 2 angir at betalingstjenestetilbyder ikke bare skal overvåke anvendelsen av sterk kundeautentisering, men også selve transaksjonen. Forordningen spesifiserer når denne overvåkingen skal skje, og hva overvåkingen skal avdekke. Videre oppstiller RTS artikkel 18 en skjerpet transaksjonsovervåkingsplikt, med krav til realtidsrisikoanalyse av transaksjonsrisikoen. Det er innholdet og rekkevidden av disse kravene jeg skal analysere nærmere i det følgende.

For å gjøre dette vil jeg først kartlegge formålet med overvåkingen (punkt 4.2). I analysen av kravene vil jeg presentere reglene for overvåkingen av autentiseringsprosedyrene (punkt 4.3), herunder kravet til dynamisk tilknytning. Hovedtyngden av analysen vil imidlertid være på overvåkingen av transaksjonen etter RTS artikkel 2 og 18 (punkt 4.4). Avslutningsvis vil jeg vurdere i hvilken grad pliktene til overvåking er egnet til å oppfylle sine formål (punkt 4.6).

4.2 Formål: Avdekke ikke godkjente betalingstransaksjoner for å forebygge og begrense omfanget av svindel

I fortalen til forordningen utdyper EBA at overvåkingen av betalingstransaksjoner skal kunne «afsløre forsøg på at gøre brug af en betalingstjenestebrugers tabte, stjålne eller uberettiget tilegnede personaliserede sikkerhedsoplysninger, og bør også sikre, at betalingstjenestebrugeren er den retmæssige bruger, som derfor giver sit samtykke til overførslen af midler og

[142] Prop.92 LS (2019–2020) s. 172-173.

adgang til sine kontooplysninger ved normal brug af de personaliserede sikkerhedsoplysninger».[143] Overvåkingen har dermed et klart svindelforebyggende formål.

At betalingsforetak bruker transaksjonsovervåkingsmekanismer til å forebygge og begrense omfanget av svindel er ikke noe nytt. Det har i en årrekke vært utviklet og tilbudt systemer for svindelovervåking i næringen. Etter det første betalingstjenestedirektivet var foretakene underlagt en overordnet plikt til å ha sikre systemer, utdypet i ikke-bindende anbefalinger.[144] Anbefalingene gjaldt både krav til risikostyring og utforming av sikkerhetssystemer til beskyttelse av kunden og betalingssystemet, herunder bruken av transaksjonsovervåkingsmekanismer. Plikten til å ha sikre systemer kunne følgelig oppfylles på mange ulike måter, men foretakene kunne ikke unnlate å implementere sikkerhets- og kontrolltiltak.

Betalingsforetak er også pålagt plikter til å håndtere operasjonell risiko og sikkerhetsrisiko.[145] Svindel er en anerkjent operasjonell risiko.[146] Etter forskrift om systemer for betalingstjenester § 2 er foretaket underlagt en forpliktelse til å avdekke «uautorisert bruk av tjenesten». På denne bakgrunn er det nærliggende å anta at betalingsforetak også før gjennomføringen av forordningen i norsk rett har brukt transaksjonsovervåking for det formål å avdekke betalingssvindel, om enn i ulik utstrekning.

At det fra norsk lovgiver og EUs side har vært ansett nødvendig å lovfeste krav til bruken av overvåkingssystemer for å sikre sterk kundeautentisering, og dermed underlegge den offentligrettslig tilsyn og kontroll, kan antas å ha flere begrunnelser. Det overordnede målet til EU med å regulere betalingsformidlingen er å fremme bruken av elektroniske betalingsløsninger.[147] En forutsetning for økt handel på tvers av landegrenser er at systemene oppleves som trygge. Spesifiseringen av overvåkingsforpliktelsene bidrar til å sikre tilliten til elektroniske betalingstransaksjoner.

Videre følger det av fortalen til PSD 2 at kravene i direktivet skal «sikre ensartet anvendelse» av EU-retten, hvor det «garanteres lige forretningsvilkår for eksisterende og nye markedsaktører». [148] Spesifiseringen av sikkerhetskravene til sterk kundeautentisering sikrer at betalingsforetakene på det europeiske markedet spiller etter samme spilleregler, og styrker dermed EUs overordnende mål om et ensartet betalingsmarked.

---

[143] RTS fortalen avsnitt (1).

[144] Europeiske sentralbanken (2014) Assessment guide for the security of internet payments.

[145] PSD 2 artikkel 95 (1).

[146] EBA/GL/2017/17, punkt 5.2 b); Basel (2001) QIS2 – Operational risk loss data, s. 6.

[147] PSD 1, fortalen avsnitt 1 og 2.

[148] PSD 2, fortalen avsnitt 6.

Videre følger det av fortalen til PSD 2 at direktivet også skal sikre «en høj grad af forbrugerbeskyttelse».[149] Når det gjelder foretakets plikter til å sikre sterk kundeautentisering er det fra en kundes perspektiv tilnærmet umulig å definere innholdet i plikten til å ha sikre systemer og selv kontrollere at den blir oppfylt. Pliktene som følger av forordningen, sikrer dermed også at innholdet i hva en kunde kan forvente av betalingsforetaket blir definert.

4.3 Plikt til å sikre «dynamisk tilknytning», jf. forskrift om systemer for betalingstjenester § 5

Det rettslige utgangspunktet for plikten til å overvåke autentiseringsprosedyrene følger av forskrift om systemer for betalingstjenester § 5 (2). I § 5 (2) heter det at «betalingstjenestetilbyderen [skal] ved elektroniske fjernbetalingstransaksjoner anvende sterk kundeautentisering som kobler transaksjonen til et spesifikt beløp og en spesifikk betalingsmottaker».[150] Det følger av ordlyden at ved initiering av elektroniske fjernbetalingstransaksjoner er det ikke tilstrekkelig å sikre at sterk kundeautentisering er benyttet.[151] Det stilles i tillegg et supplerende krav til at kundeautentiseringen, transaksjonen og betalingsmottakeren er tilknyttet hverandre. Det nærmere innholdet i det supplerende sikkerhetskravet følger av RTS artikkel 5, formulert som et krav til «dynamisk tilknytning».

Det følger av RTS artikkel 5 (1) at betaleren skal «gøres opmerksom» på betalingstransaksjonsbeløpet og på betalingsmottakeren,[152] og at «autentifikationskoden» som betalingstjenestetilbyderen har godkjent «svarer til det oprindelige specifikke betalingstransaktionsbeløb og til identiteten af den betalingsmodtager, som betaleren har godkendt».[153] Bakgrunnen for sikkerhetskravene til dynamisk tilknytning er at elektroniske betalingstransaksjoner innebærer større risiko for svindel.[154] Dersom det ikke er dynamisk tilknytning er det rimeligvis risiko for at transaksjonen ikke er godkjent av kunden, jf. formålet med sikkerhetskravene i forordningen.

Kravet til dynamisk tilknytning i RTS artikkel 5 reiser noen tolkningsspørsmål. For det første er det spørsmål om hva en «autentifikationskode» er. Autentifikasjonskoden er regulert i RTS artikkel 4, som fastslår at ved anvendelse av sterk kundeautentifikasjon skal «autentifikationen være baseret på to eller flere elementer, der karakteriseres som viden, besiddelse og iboende egenskab, og skal føre til generering af en autentifikationskode». Autentifikasjonskode er følgelig en kode som genereres i forbindelse med autentiseringen av kunden, og vil genereres i forbindelse med bruken av løsning for sterk kundeautentisering.

[149] PSD 2, fortalen avsnitt 6.
[150] Gjennomfører RTS artikkel 5.
[151] EBA/Op/2019/06, avsnitt 37.
[152] RTS artikkel 5(1)(a).
[153] RTS artikkel 5(1)(c).
[154] RTS, fortalen avsnitt 3.

Siden sterk kundeautentisering skal anvendes til å avgi samtykke til initiering av betalingstransaksjonen, vil autentifikasjonskoden genereres i forbindelse med at betaleren autentiserer at betaleren er den vedkommende utgir seg for å være *og* bruker det bestemte betalingsinstrumentet til å avgi samtykke til initiering av betalingstransaksjonen. I Norge vil det som regel være BankID som brukes som løsning for sterk kundeautentisering, og være løsningen som generer slik autentifikasjonskode.

Det neste spørsmålet er i hvilket tidsrom plikten til dynamisk tilknytning gjelder. Det følger av RTS artikkel 5 (2) at både a) «transaktionsbeløbet og betalingsmodtageren» og b) «de oplysninger, som vises betaleren» skal garanteres «i alle autentifikationsfaserne». Det følger av ordlyden at kravet til dynamisk tilknytning må være oppfylt gjennom hele prosessen med å gjennomføre en betalingstransaksjon. Med andre ord inkludert generering av autentifikasjonskode, formidlingen av koden, og bruken av koden.[155]

Et tredje spørsmål er hvordan kravet til dynamisk tilknytning skal sikres. Det følger av artikkel 5 (2) at de ulike elementene skal garanteres gjennom «sikkerhetsforanstaltninger». Ordlyden oppstiller dermed krav til sikkerhetstiltak på betalingstjenesteyters side, men presiserer ikke hvilke sikkerhetstiltak som kreves.[156] Det følger allikevel i artikkel 5 (2) at sikkerhetstiltakene må være egnet til å sikre «fortroligheden, ægtheden og integriteten» til de ulike elementene i kravet til dynamisk tilknytning.

Når det gjelder tilknytningen mellom autentifikasjonskoden, transaksjonsbeløpet og betalingsmottaker, jf. RTS artikkel 5 (2)(a), kan det legges til grunn at det mest praktiske sikkerhetstiltaket er bruk av elektroniske overvåkingsmekanismer. Det innebærer at betalingsforetaket må overvåke transaksjonens beløp og betalingsmottaker fra kunden initierer betalingen helt frem til transaksjonen er ferdig gjennomført, samt sikre at opplysningene som vises til kunden samsvarer med disse. Overvåkingen skal i tråd med kravet til dynamisk tilknytning avdekke endringer i transaksjonsbeløpet og betalingsmottaker etter autentifikasjonskoden er blitt generert. Det innebærer også at overvåkingen av autentiseringsprosedyren skjer i alle fasene av autentiseringsprosessen.

Når det gjelder sikkerhetskravene for å sikre «de oplysninger, som vises betaleren», jf. artikkel 5 (2)(b) er det et tolkningsspørsmål om hvilke krav som stilles til hvordan opplysningene skal «vises betaleren». Det følger av ordlyden «vises betaleren» at opplysningene må dukke opp og

[155] EBA-2020-5366.
[156] EBA-2020-5366.

være synlige for betaleren i forbindelse med at kunden samtykker til betalingen. EBA har presisert at med «betaleren» i artikkel 5 menes innehaver av kontonummeret tilknyttet kontoen som skal belastes.[157] Det følger av dette at innehaver av kontonummeret skal få synlige opplysninger om betalingsbeløpet og betalingsmottaker.

Det at «fortroligheden, ægtheden og integriteten» til opplysningene må være sikret, krever videre at opplysningene er gitt på en trygg måte. Ut over det gir ordlyden liten veiledning om hvordan opplysningene skal gjøres synlige. EBA har imidlertid presisert at «it is not required that the authentication code is computed on and dynamically linked to the payer's device».[158] Opplysningene kan eksempelvis gis på SMS.[159] Det vil formodentlig også være tilstrekkelig at opplysningene fremgår av nettleseren i forbindelse med autentifikasjonsprosedyren. Det følger av dette at hvordan betaleren «gøres opmerksom» på opplysningene, jf. RTS artikkel 5 (1)(c), avhenger av de tekniske løsningene for kundeautentiseringen.

Betydningen av plikten til dynamisk tilknytning er at tredjeparter som opererer under PSD 2 blir forhindret fra å misbruke adgangen til å få tilgang på betalerens konto gjennom kontotilbyders API med hensikt å manipulere initieringen av betalingstransaksjoner.[160] Et annet poeng er at plikten til å gjøre kunden oppmerksom på transaksjonsbeløpet og betalingsmottaker kan avverge betaleren fra å i det hele tatt samtykke til svindelhenvendelser. Ved å opplyse kunden om transaksjonsbeløpet og betalingsmottaker får betaleren presumptivt mulighet til å vurdere om vedkommende faktisk skal samtykke til den forestående betalingstransaksjonen.

Der kunden er utsatt for phishing, og bruker sine sikkerhetsopplysninger tilknyttet BankID på en falsk nettside, er det imidlertid et spørsmål om kravet til dynamisk tilknytning sikrer at det faktisk er innehaver av kontonummeret (og følgelig innehaver av BankID) som «gøres opmerksom» på opplysningene, jf. RTS artikkel 5 (1)(c). Der opplysningene om betalingbeløpet og betalingsmottaker vises i nettleseren i forbindelse med autentifikasjonsprosedyren er det en risiko for at det er svindler, som sitter med den ekte autentifikasjonssiden, som får oppgitt opplysningene. Det kan av den grunn stilles spørsmålstegn ved hvor egnet kravet til sterk kundeautentisering – og herunder kravet til dynamisk tilknytning, er på å avverge denne typen svindelhenvendelser.

Det fjerde og siste spørsmålet er hva som er rekkevidden av plikten til å sikre dynamisk tilknytning. Som analysen over har vist er dynamisk tilknytning et supplerende krav til anvendelsen

[157] EBA-2019-4556.

[158] EBA-2020-5366.

[159] EBA-2018-4414.

[160] Som eksempelvis ved såkalt «man-in-the-middle»-angrep, jf. Conti, Dragoni, Lesyk (2016) s. 2027–2051.

av sterk kundeautentisering ved initiering av elektroniske betalingstransaksjoner. Rekkevidden av kravet til dynamisk tilknytning er dermed sammenfallende med rekkevidden til kravet om å anvende sterk kundeautentisering.

Plikten til å anvende sterk kundeautentisering ved initiering av elektroniske betalingstransaksjoner er imidlertid ikke absolutt.[161] I forordningens kapittel III følger de nærmere vilkårene for å gjøre unntak. Om betalingstjenesteyter benytter seg av et av unntakene fra kravet til sterk kundeautentisering vil kundens samtykke til transaksjonen ikke generere en autentifikasjonskode som nevnt i forordningens artikkel 4. Da vil nødvendigvis også plikten til å sikre dynamisk tilknytning mellom autentifikasjonskoden, transaksjonsbeløpet og betalingsmottaker bortfalle.[162]

4.4 Plikt til å overvåke «brug af personaliserede sikkerhedsoplysninger», jf. RTS artikkel 2

Det rettslige utgangspunktet for plikten til å anvende transaksjonsovervåkingsmekanismer følger av RTS artikkel 2 (1), som krever bruk av «transaktionsovervågningsmekanismer, som sætter dem i stand til at afsløre uautoriserede eller svigagtige betalingstransaktioner med henblik på at gennemføre de sikkerhedsforanstaltninger, der er omhandlet i artikel 1, litra a) og b)». Det følger av første ledd annet punktum at overvåkingsmekanismene skal være basert på en analyse av betalingstransaksjoner «under hensyntagen til elementer, som er typiske for betalingstjenestebrugere i forbindelse med normal brug af personaliserede sikkerhedsoplysninger». I lys av formålet med overvåkingen er det naturlig å tolke ordlyden dithen at overvåkingen skal avdekke avvik fra normal bruk av personlige sikkerhetsopplysninger. Forutsetningsvis kan unormal bruk av personlige sikkerhetsopplysninger indikere ikke godkjente betalingstransaksjoner og svikaktige betalingstransaksjoner.

Et første spørsmål er tidspunktet for overvåkingen etter RTS artikkel 2. Ordlyden i artikkel 2 angir ikke når foretaket skal gjennomføre transaksjonsovervåkingen. Spørsmålet om tidspunktet for transaksjonsovervåking etter RTS artikkel 2 er imidlertid blitt reist i en Q&A til EBA i spørsmål 2018-4090.[163] EBA uttaler at overvåkingen etter artikkel 2 «is usually carried out "after" the execution of the payment transaction». Uttalelsen fastslår at det ikke kreves at overvåkingen skjer i sanntid, og at det er tilstrekkelig at overvåkingen er en etterhåndskontroll.

Det neste spørsmålet er hva overvåkingen innebærer. Det at betalingsforetaket etter ordlyden skal ta hensyn til elementer som er «typiske for betalingstjenestebrugere» innebærer etter en

[161] RTS artikkel 1 (b), jf. fortalen avsnitt 9.

[162] EBA-2020-5673.

[163] EBA-2018-4090.

naturlig språklig forståelse at foretaket må ha kjennskap til hva som er typisk for normal bruk av personlige sikkerhetsopplysninger. Dermed oppstilles også krav til at betalingsforetak lagrer opplysninger om hvordan betalingstjenestebrukere bruker de personlige sikkerhetsopplysningene for det formål å finne mønstre i hvordan de typisk brukes.

I artikkel 2 (2) presiserer forordningen videre krav til at «transaktionsovervågningsmekanismen som et minimum tager højde for» hver av de følgende risikobaserte faktorer:

> «a) lister over svækkede eller stjålne autentifikasjonselementer
> b) de enkelte betalingstransaktionsbeløb
> c) kende scenarier for svig i forbindelse med udbud af betalingstjenester
> d) tegn på malware-infektion i autentifikationsprocuderens sessioner
> e) hvis betalingstjenesteudbyderen stiller adgangsanordning eller software til rådighed, en log over brugen af den adgangsanordning eller det software, som er stillet til rådighed for betalingstjenestebrugeren, og unormal brug af adgangsanordning eller software».

Av sammenhengen følger det at listen angir tilfeller hvor det foreligger elementer ved initieringen av en betalingstransaksjon som ikke er «typiske for betalingstjenestebrugere i forbindelse med normal brug af personaliserede sikkerhedsoplysninger», og som dermed kan indikere at transaksjonen ikke er godkjent.[164] Da listen angir et minimum av risikofaktorer som betalingsforetakene skal ta høyde for, er listen ikke uttømmende. Betalingsforetak kan med utgangspunkt i artikkel 2 overvåke for flere risikofaktorer som er egnet til å avdekke unormal bruk av de personlige sikkerhetsopplysningene.

Listen over risikofaktorer innebærer at foretakene må innrette systemet slik at det er egnet til å utløse alarm dersom en transaksjon faller inn under en eller flere av faktorene. Noen av risikofaktorene fremstår som sjekklister, som eksempelvis «lister over svækkede eller stjålne autentifikasjonselementer», jf. artikkel 2 (2)(a). Det følger ikke av ordlyden hvordan foretaket skal gå frem for å inneha denne typen opplysning. Foretaket kan rimeligvis enten selv eller i samarbeid med øvrige betalingstjenestetilbydere utarbeide 'svartelister'. Andre risikofaktorer, slik som «kende scenarier for svig i forbindelse med udbud af betalingstjenester», jf. artikkel 2 (2)(c), innebærer at foretaket må utarbeide 'scenarioer' som kan koble transaksjonen sammen med risikofaktoren.

Risikofaktorer angir opplysninger av generell karakter som for alle betalingstjenestebrukere kan indikere unormal bruk av de personlige sikkerhetsopplysningene. Det reiser et tolkningsspørsmål om betalingsforetaket også er pliktig til å vite hva som er normal bruk av personlige

[164] RTS artikkel 2 (1).

sikkerhetsopplysninger for den enkelte kunde. I forlengelsen av det, om det er grunnlag i artikkel 2 for å kreve at betalingsforetakene individualiserer utarbeidelsen av scenarioer i overvåkingssystemet.

Dersom overvåkingen av transaksjoner individualiseres til den enkeltes kundes bruk av personlige sikkerhetsopplysninger kan overvåkingen eksempelvis avdekke dersom personlige passord tastes inn etter et annet mønster enn kunden alminnelig bruker, og dersom passordet brukes fra en annen IP-adresse eller fra et annet brukersted enn det som er normalt for kunden. En slik plikt vil pålegge betalingsforetaket relativt langtrekkende plikter til informasjonsinnhenting av hver enkelt kundes adferdsmønster i bruk av de personlige sikkerhetsopplysningene. Til gjengjeld kan det argumenteres for at individualisert overvåking vil gjøre betalingsforetakene best rustet til å avdekke ikke godkjente eller svikaktige betalingstransaksjoner, som er formålet med overvåkingen.

Det følger av ordlyden i den svenske språkdrakten at overvåkningen skal ta hensyn til «element som är typiska för betaltjänstanvändaren vid normal användning av personliga säkerhetsbehörighetsuppgifter». Den engelske bruker ordlyden «elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials». Både den svenske og den engelske ordlyden bruker bestemt form. Bruken av bestemt form indikerer at overvåkingen skal ta i betraktning elementer som er typiske for betalingstjenestebrukeren i dennes normale bruk av de personlige sikkerhetsopplysningene. Det kan tas til inntekt for at reglene i transaksjonsovervåkingen må tilpasses kontekstuelle adferdsmessige karakteristikker ved den enkelte kunde.

Tolkningen underbygges av uttalelser fra EBA fra 2022.[165] På avsnitt 326 uttaler EBA at

> «[s]ome market participants argued that behavioural characteristics related to the environmental analysis and payment habits, such as those related to location of the PSU [payment service user], time of transaction, device being used, spending habits, online store where the purchase is carried out, should qualify as inherence. In line with the above clarifications, the EBA has shared the view that while these contribute to improving the security of payment transactions and data, they can be viewed in the light of the transaction monitoring mechanisms under Article 2 of the RTS on SCA&CSC or under the transaction risk analysis exemption from SCA under Article 18 of the same RTS. These behavioural characteristics do not relate to a physical property of the body and thus cannot be considered as an inherence SCA element».

[165] EBA/Op/2022/06.

Uttalelsen knytter seg til et spørsmål om hvordan betalingstjenesteyter kan sikre elementet «besittelse» for å oppfylle kravet til sterk kundeautentisering. EBA bruker innholdet i overvåkingsforpliktelsen i artikkel 2 og artikkel 18 som et tolkningsmoment. Uttalelsen har dermed også relevans for fastleggelsen av innholdet overvåkingsforpliktelsen. Som det følger av uttalelsen forutsetter EBA at transaksjonsovervåkingen etter artikkel 2 og artikkel 18 tar høyde for adferdsmessige karakteristikker tilknyttet miljøanalyse og betalingsvaner, som plasseringen av betalingstjenestebrukeren, tidspunktet for transaksjonen, enheten som brukes, forbruksvaner og nettbutikken hvor kjøpet utføres fra. Den type overvåking EBA forutsetter at foretaket utfører etter artikkel 2 og 18 innebærer nødvendigvis at overvåkingen er tilpasset den enkelte kunde. Det er dermed grunnlag for å konkludere at overvåkingen skal tilpasses den enkelte kunde, og skal avdekke avvikende kundeadferd. Uttalelsen til EBA angir videre veiledning om hvordan overvåkingen kan individualiseres.

Det neste spørsmålet er hvor spesifisert den kundespesifikke overvåkingen må være. Det kan argumenteres for at en høy grad av individualisering av reglene opp mot den enkelte kunde vil være en effektiv måte å avdekke avvikende adferd, herunder være effektiv til å avdekke initieringen av ikke godkjente betalingstransaksjoner. Høy grad av individualisering vil imidlertid være tidkrevende og kreve at betalingsforetakene samler inn og analyserer store mengder av opplysninger om kunden.[166]

Sett hen til antallet svindeltransaksjoner tross alt utgjør en relativ liten andel av den totale summen transaksjoner som blir initiert, vil for høye krav til individualisering i transaksjonsovervåkingen nok stride imot det reviderte betalingstjenestedirektivets andre hensyn, som er effektivitet i betalingsformidlingen. På den andre siden kan reglene heller ikke være for generelle. Dersom reglene og scenarioene er for generelle vil systemet generere for mange falske positiver, noe som blir tidkrevende for betalingsforetaket å håndtere. Dette vil også kunne stride mot hensynet til effektivitet i betalingsformidlingen. På den bakgrunn kan det antas at det er sentralt for foretaket å oppnå en balansegang mellom hensynet til effektivitet og beskyttelse av kunden når foretaket skal utarbeide scenarioer i overvåkingen. Analysen indikerer imidlertid at det nok vil initieres noen ikke godkjente betalingstransaksjoner som ikke blir fanget opp av overvåkingen.

Det neste spørsmålet er rekkevidden av plikten til å anvende transaksjonsovervåkingsmekanismer. Som det fremgår av ordlyden i artikkel 2 er plikten til å anvende transaksjonsovervåkingsmekanismer i artikkel 2 en presisering av kravet til sterk kundeautentisering. Til forskjell fra

[166] Det kan i den forbindelse også oppstå personvernspørsmål, se eksempelvis Marasa (2020) s. 629; Nærmere drøftelse av personvernimplikasjoner under PSD 2 vil ikke bli behandlet i denne avhandlingen.

kravet til å overvåke autentiseringsprosedyren er rekkevidden av transaksjonsovervåkingsplikten oppstilt i artikkel 2 etter sin ordlyd imidlertid ikke avhengig av om det gjøres unntak fra kravet til sterk kundeautentisering. Plikten til transaksjonsovervåking rekker følgelig ut over den sikkerheten som kravet til sterk kundeautentisering tilbyr. Dette er også lagt til grunn av EBA.[167]

Det at transaksjonsovervåkingen rekker lenger enn kravet til sterk kundeautentisering sammenfaller også med det overordnede formålet med sikkerhetskravene, som er å avdekke ikke godkjente betalingstransaksjoner. Svindelmetodene benyttet av de kriminelle kan endre seg med tiden, og omfatter et mangfold av praksis og teknikker. Metodene kan eksempelvis innebære alt fra tyveri av autentiseringslegitimasjon, fakturatukling og sosial manipulasjon. Foretakene er videre pålagt krav til revisjon av etterlevelsen etter RTS artikkel 3, som sikrer kontinuerlig forbedring av systemene. Det viser at transaksjonsovervåkingen er ment å være dynamisk av karakter med formål å avdekke utvikling i kriminalitetsbilde som ikke fanges opp av kravet til sterk kundeautentisering.

4.5 Plikt til å gjøre «realtidsanalyse af risici», jf. RTS artikkel 18 (TRA-unntaket)

Som analysen ovenfor har vist er kravet til sterk kundeautentisering, herunder kravet til dynamisk tilknytning etter RTS artikkel 5, og transaksjonsovervåkingsplikten etter RTS artikkel 2, basiskravene for sikkerhet ved initieringen av elektroniske betalingstransaksjoner. I tillegg til basiskravene oppstiller forordningens artikkel 18 krav til transaksjonsovervåking dersom betalingsforetaket ønsker å gjøre unntak fra kravet til sterk kundeautentisering basert på en vurdering av transaksjonens «risiko». Dette risikobaserte unntaket fra kravet til sterk kundeautentisering kommer i tillegg til de regelbaserte unntakene i artikkel 10 til 17, og omtales ofte som Transaction Risk Analysis-unntaket («TRA»-unntaket).

Det følger av artikkel 18 at unntaket kan anvendes dersom risikoen ansees for å være «lav». Hvorvidt risikoen er «lav» skal etter bestemmelsen vurderes på bakgrunn av bruk av transaksjonsovervåkingsmekanismer. Det følger av ordlyden at bestemmelsen sikter til bruk av transaksjonsovervåkingsmekanismene angitt i forordningens artikkel 2, som redegjort for ovenfor. I tillegg oppstiller artikkel 18 (2)(c) ytterligere krav til bruk av en skjerpet overvåkingsmekanismene etter en «realtidsanalyse af risici». I det følgende vil jeg se nærmere på hva denne realtidsrisikovurderingen innebærer, og forholdet mellom overvåkingen etter artikkel 2 og 18.

(i) Realtidsrisikoanalysen etter TRA-unntaket

[167] 2023/0210 (COD), avsnitt 100.

For det første er det spørsmål når risikovurderingen skal gjennomføres. Det følger av ordlyden «realtidsanalyse af risici» at risikovurderingen utføres i sanntid. Realtidsanalysen gir adgang til å gjøre unntak fra sterk kundeautentisering. Sett hen til at sterk kundeautentisering skal sikres i forbindelse med kundens samtykke må risikovurderingen nødvendigvis utføres før transaksjonen er autorisert.[168]

Det neste spørsmålet er hvordan risikovurderingen skal gjennomføres. Av artikkel 18 (2)(c) følger det at risikoen ansees for å være «lav» dersom realtidsanalysen ikke konstaterer følgende

> «i) unormale udgifts- eller adfærdsmønstre hos betaleren
> ii) usædvanlige oplysninger om betalerens adgang til anordninger og software
> iii) malware-infektion i autentifikationsprocedurens sessioner
> iv) kendte scenarier for svig i forbindelse med udbud af betalingstjenester
> v) unormalt opholdssted for betaleren
> vi) højrisikoopholdssted for betalingsmodtageren.»

For å kunne anvende det risikobaserte unntaket for sterk kundeautentisering må alle disse nevnte risikofaktorene kombineres til en risikoberegning for hver enkelt transaksjon.[169] Det stilles forutsetningsvis krav om at foretaket har terskelverdier for betalerens normale utgift- og handlemønster, hvordan betaleren normalt har adgang til anordninger og software, hvor betaleren normalt oppholder seg når betalinger initieres, samt hvilke oppholdssteder for betalingsmottakere som innebærer høy risiko. Disse terskelverdiene må innarbeides i systemene, sånn at avvik avdekkes i transaksjonsovervåkingen.

Det kan imidlertid tenkes at en betalingstjenesteyter ikke har tilstrekkelig informasjon om betaleren til å identifisere risiko tilknyttet de seks opplistede risikofaktorene. Utfordringen kan tenkes å være aktuell i kortvarige kundeforhold. Mellom en betaler og en tredjepart kan kundeforholdet være avgrenset til gjennomføring av en enkeltstående transaksjon. Dersom tredjeparten benytter gateway-leverandører,[170] som visa og mastercard, kan det videre tenkes at gateway-leverandøren ikke gir de relevante opplysningene til tredjeparten som ønsker å benytte seg av TRA-unntaket. I nevnte tilfeller har betalingstjenesteyteren begrenset informasjon om transaksjonsmiljøet og annen relatert informasjon.

---

[168] EBA-2018-4090.

[169] RTS artikkel 18 (3).

[170] En gateway-leverandør er en tjenesteleverandør for e-handelsapplikasjoner som tilbyr verktøy for å behandle en betaling mellom en kunde, forhandler og banker over internett. Leverandøren beskytter betalingsinformasjon ved å kryptere sensitiv informasjon, for eksempel kreditt-/debetkortdetaljer, for å sikre at informasjon sendes sikkert mellom en kunde og betalingsbehandleren, jf. Oo (2019) s. 1329-1334.

Spørsmål om betalingstjenesteytere er underlagt forpliktelse til å innhente opplysninger om betaleren fra andre betalingstjenesteytere er blitt reist til EBA.[171] EBA uttaler at betalingstjenesteyter er forventet å sjekke «as far as it possibly can» hvorvidt en av de seks risikofaktorene er til stede. Ved mangel på opplysninger uttaler EBA at betalingstjenesteyter «should consider requesting information from another PSP in the payment chain». EBA fremhever følgelig muligheten for å be om opplysninger om betaleren fra andre betalingstjenesteytere. Uttalelsen kan imidlertid ikke tas til inntekt for at betalingstjenesteyter har plikt til å innhente nødvendige opplysninger fra andre betalingstjenesteytere, selv om det innebærer at betalingstjenesteyter ikke har tilstrekkelig informasjon til å identifisere at ingen av de seks risikofaktorene er til stede.

I tillegg til at realtidsvurderingen må påvise lav risiko, må foretaket kunne påvise at svindelraten i foretaket er tilsvarende eller under terskelverdiene fastsatt i vedlegget til forordningen.[172] Videre må transaksjonsbeløpet i hvert enkelt tilfelle ikke overstige terskelverdiene fastsatt i vedlegget til forordningen.[173] Unntaket i artikkel 18 kommer følgelig først til anvendelse dersom transaksjonsrisikoen er lav, og de øvrige vilkårene angitt i artikkel 18 er til stede.

Spørsmål om beregning av svindelraten er reist flere ganger til EBA.[174] De mest sentrale uttalelsene fra EBA er at svindelraten ikke bare inkluderer ikke godkjente transaksjoner, men også andre svindeltransaksjoner som følge av manipulasjon av betaleren.[175] I uttalelse fra 2018 klargjør EBA videre at for transaksjoner behandlet av flere betalingstjenesteytere, slik som ved korttransaksjoner, skal de ikke godkjente transaksjonene som inngår i svindelraten omfatte (i) de ikke godkjente transaksjonene den gitte betalingstjenesteyter har båret ansvar for etter tapsfordelingsreglene i samsvar med PSD artikkel 74, og (ii) andre svindeltransaksjoner som ikke er blitt forhindret av betalingstjenesteyteren.[176]

Det følger av det overnevnte at det stilles betydelige krav til implementering av sikkerhetsmekanismer og overvåking for at betalingsforetak kan anvende TRA-unntaket. Av sammenhengen gir også det mening. Kravet til sterk kundeautentisering i PSD artikkel 97 er fra EUs side ment som et av de viktigste tiltakene for å forhindre svindel. Om det skal gjøres unntak fra dette kravet må betalingsforetaket kunne vise at det ikke er nødvendig at kunden går gjennom ekstra sikkerhetssteg for å initiere betalingstransaksjonen. At unntaksadgangen fra kravet til sterk kundeautentisering skal være snever er også fremhevet av EBA i arbeidet med forordningen, hvor EBA som svar på høringsrunden uttaler følgende

[171] EBA-2018-4127.
[172] RTS artikkel 18 (2)(a).
[173] RTS artikkel 18 (2)(b).
[174] Se eksempelvis EBA- 2018-4032, EBA-2018-4034, EBA-2018-4044, og EBA-2019-4702.
[175] EBA/CP/2017/13.
[176] EBA/2018/Op/04, avsnitt 46.

> «any exemption that would allow the majority of payments to be exempted from SCA would go against PSD2's objective of enhancing security, and against the definition of an exemption».[177]

TRA-unntaket er drevet frem av næringen selv. I det første forslaget til forordningen foreslo EBA kun regelbaserte unntak.[178] Årsaken var at EBA i arbeidet med utkastet ikke hadde identifisert legitime objektive kriterier for et risikobasert unntak.[179] Forslaget avvek imidlertid fra EBA's tidligere anbefalinger under det første betalingstjenestedirektivet, hvor sterk kundeautentisering ikke ble anbefalt som nødvendig dersom risikoen for svindel var lav. Forslaget til EBA skapte derfor stor diskusjon i næringen, og i høringsrunden til forslaget ble det reist mange spørsmål om unntakenes rekkevidde, samt et ønske fra næringen om å unnta sterk kundeautentisering etter en risikovurdering.[180]

I høringsrunden til forordningen fremhever til illustrasjon Finans Norge at svindelmetoder er i rask utvikling, med den følge av en lovfestet detaljert liste kan bli utdatert.[181] En risikobasert tilnærming vil til sammenligning kunne dynamisk tilpasses nye svindelmetoder. Videre fremhever Finans Norge det store omfanget data som kontotjenestetilbyder har, som kan brukes til å utarbeide forståelse av risiko tilknyttet autentifiseringsprosessen og betalingstransaksjonen. Kontotjenestetilbydere er presumtivt egnet til å vurdere risikoen for svindel.

I arbeidet med forslaget om risikobasert unntak sto EBA overfor en vanskelig balansegang mellom konkurrerende hensyn.[182] På den ene siden står hensynet til strenge sikkerhetsstandarder, som taler for høy grad av regulering for å unngå omgåelse av regler, samt at den enkelte betalingsbruker bør være underlagt flere sikkerhets- og autentifikasjonsprosedyrer. På den andre siden står markedshensyn som taler for fleksibilitet i reguleringen og minimalt med prosedyrer for den enkelte kunde å gjennomgå. Etter høringsrunden sa EBA seg imidlertid enige i noen av forslagene reist av markedsaktører i høringsrunden, og gjorde flere endringer i utkastet.[183] Det resulterte blant annet i TRA-unntaket i artikkel 18.

(ii) Forholdet mellom transaksjonsovervåkingen i artikkel 2 og TRA-unntaket i artikkel 18

---

[177] EBA/RTS/2017/02, avsnitt 20.

[178] EBA (2016). Public Hearing on strong customer authentication & secure communication (SCA & CSC) under Aricle 97 PSD2, s. 19.

[179] EBA/RTS/2017/02, avsnitt 20.

[180] EBA/RTS/2017/02, avsnitt 19.

[181] https://www.eba.europa.eu/node/81948/submission/560.

[182] EBA/Op/2017/09 s. 2.

[183] EBA/RTS/2017/02, avsnitt 26.

Både artikkel 2 og 18 forplikter betalingsforetaket til å anvende transaksjonsovervåkingsmekanismer. Det er imidlertid noen sentrale forskjeller både i innholdet og anvendelsesområde til de to bestemmelsene.

For det første er tidspunktet for overvåkingen ulik. Overvåkingen etter artikkel 18 kommer i stedet for anvendelse av sterk kundeautentisering, og er følgelig ment å autentisere kunden ved initiering av den elektroniske betalingstransaksjonen. Som avdekket av analysen av artikkel 2 vil overvåkingen etter denne bestemmelsen ofte gjennomføres som en etterhåndskontroll av gjennomførte transaksjoner.

For det andre er rettsvirkningene av avdekkede funn i overvåkingen etter de to bestemmelsene ulik. Avvik fra de kundespesifikke opplysningene innebærer etter artikkel 18 at transaksjonsrisikoen for svindel ikke er lav. Det at risikoen ikke er lav innebærer at foretaket ikke kan gjøre unntak fra kravet til sterk kundeautentisering. Følgelig vil funn i overvåkingen medføre at foretaket allikevel må oppfylle kravet til sterk kundeautentisering. Til sammenligning vil funn i overvåkingen etter artikkel 2 etter sitt formål indikere at transaksjonen ikke er godkjent av kunden.[184]

Foretakene som benytter seg av TRA-unntaket må nødvendigvis foreta en realtidsrisikoanalyse av initieringen av alle elektroniske fjernbetalingstransaksjoner, for å undersøke om vilkårene er oppfylt i et konkret tilfelle. Denne risikovurderingen vil komme i tillegg til transaksjonsovervåkingen foretaket er forpliktet til å anvende etter artikkel 2. For de foretakene som i sin drift ikke velger å benytte adgangen til det risikobaserte unntaket, vil imidlertid ikke plikten til å foreta realtidsrisikovurdering etter artikkel 18 gjøre seg gjeldende. Den praktiske betydningen av dette er at det bare er foretakene som velger å benytte seg av unntaket i artikkel 18 som er underlagt den mer detaljerte og skjerpede svindelovervåkingen, samt plikten til å vurdere transaksjonsrisikoen på bakgrunn av foretakets svindelrate.

For de betalingsforetakene som velger å benytte seg av det risikobaserte unntaket får overvåkingsplikten i artikkel 2 betydning ut over sitt angitte anvendelsesområde. Transaksjonsovervåkingen etter artikkel 2 er et viktig kunnskapsgrunnlag for å holde oppsyn med om svindelraten til foretaket er innenfor svindelratene angitt i vedlegget til forordningen. Samlet sett illustrerer forholdet mellom artikkel 2 og artikkel 18 at rekkevidden av pliktene pålagt det enkelte betalingsforetak er avhengig av hvordan betalingsforetaket har valgt å organisere driften av sin virksomhet.

[184] For nærmere redegjørelse av betydningen av funn fra overvåkingen, se del III.

4.6 Er overvåkingsforpliktelsene egnet til å oppfylle sine formål?

4.6.1 Overvåkingsforpliktelsenes klarhet og tilgjengelighet

Når det gjelder overvåkingsforpliktelsenes klarhet er det nærmere innholdet i pliktene presisert i en rekke uttalelser fra EBA. Som uttalelsen fra EBA i 2019 gir uttrykk for var det i tiden etter implementeringen av kravet til sterk kundeautentisering, varierende grad av etterlevelse i EUs medlemsstater.[185] Det at det har vært et utstrakt behov for presiseringer kan i seg selv antyde at pliktenes innhold ikke er tilstrekkelig klart. I tillegg medfører mangfoldet av presiseringer fra EBA at rettskildebildet i fastleggelsen av pliktenes presise innhold blir mer komplekst. Det kan svekke muligheten til å gjøre seg kjent med pliktens innhold.

Tross utfordringene med å implementere sikkerhetskravene fant Den europeiske kommisjonen i evalueringsrapporten av PSD 2,[186] publisert i juni 2023, at kravet til sterk kundeautentisering har hatt en betydelig svindelreduserende effekt.[187] Rapporten peker imidlertid også på at til tross for at volumet av svindeltransaksjoner har gått ned etter implementeringen av sterk kundeautentisering, har nye former for betalingssvindel oppstått.

Særlig er det en økende trend med phishingtransaksjoner, samt betalingstransaksjonen som betaler selv er lurt til å autorisere gjennom sosial manipulering (autorisert betalingssvindel). Det uttales at sterk kundeautentisering ikke er egnet til å fange opp nye typer svindeltransaksjoner, da de ofte er godkjent og autentisert av kunden selv eller av svindler ved bruk av kundens løsning for sterk kundeautentisering. For å avdekke denne typen svindel er betalingsforetaket avhengig av at transaksjonen blir avdekket i transaksjonsovervåkingen. Transaksjonsovervåkingen får dermed en helt sentral betydning i svindelforebyggingen.

Som avdekket i analysen er formålet med den overordnede transaksjonsovervåkingsforpliktelsen i RTS artikkel 2 «å afsløre uautoriserte og svigagtige betalingstransaktioner». En innvending er at ordlyden «uautorisert» kan gi et feilaktig inntrykk av at det hovedsakelig er autentiseringsprosedyren som skal overvåkes. Følgelig, at transaksjonsovervåkingen i hovedsak skal avdekke tilfeller hvor det er synbart for betalingsforetaket at kunden ikke er korrekt autentisert, og at transaksjonen på den bakgrunn ikke er godkjent. En slik tolkning vil imidlertid være en feilslutning.

Etter artikkel 2 skal foretaket også overvåke for å avdekke ikke godkjente transaksjoner der transaksjonen tilsynelatende er godkjent og autentisert av betaleren. Rent praktisk må betalingsforetaket «flagge» svindeltransaksjoner, og disse kan i etterkant vise seg både å være godkjent

[185] EBA/Op/2019/06, avsnitt 11 fl.
[186] SWD 2023/231 final.
[187] SWD 2023/231 final, s. 117.

og ikke godkjent av kunden. Både avdekkede ikke godkjente transaksjoner og autoriserte svindeltransaksjoner skal videre registreres og inngå i svindelraten, jf. vurderingen ovenom om beregning av svindelraten. En risiko ved ordlyden i RTS artikkel 2 er at den ikke tilstrekkelig synliggjør dette. Dersom foretak ikke er klar over denne forpliktelsen innebærer det fare for følgefeil der foretaket ikke avdekker – og følgelig heller ikke undersøker, alarmer om svindeltransaksjoner autentisert med sterk kundeautentisering.

Rapporten til den Europeiske kommisjonen indentifiserer derfor at risikoen for svindel, herunder kunders tap av tillit til betalinger som følge av svindelrisikoen, fortsetter å være en av nøkkelutfordringene i betalingssystemet.[188] Et velfungerende betalingssystem er avhengig av kundenes tillit.[189] Tap av tillit kan i ytterste konsekvens undergrave det overordnede formålet med betalingstjenestedirektivet, som er fremme det elektroniske betalingssystemet.

Som også fremhevet av Høyesterett i HR-2022-2468-A vil det være skadelig for tilliten til digitale banktjenester og digitale tjenester mer generelt om det blir for enkelt å gjennomføre bedrageri.[190] Særlig der BankID misbrukes, er spørsmålet om digital tillit særdeles viktig. I tillegg til å være et betalingsinstrument bruker BankID også til flere sentrale offentlige register og tjenester. Som fremhevet av Økokrim, «[h]vis det blir vanskelig å skille mellom hva som er legitim bruk av BankID, og hva som ikke er det, kan det raskt medføre utfordringer i kommunikasjonen mellom befolkningen og det offentlige».[191]

Økningen av autorisert betalingssvindel er en av årsakene til at kommisjonen sommeren 2023, publiserte forslag til nye forordninger som skal gjelde i stedet for nåværende betalingstjenestedirektiv.[192] Forslaget innebærer blant annet å utvide transaksjonsovervåkingspliktens formålsbeskrivelse til å ha et generelt svindelforebyggende formål.[193] Plikten til å anvende transaksjonsovervåkingsmekanismer i forslaget til den nye forordningen håndterer flere av svakhetene avdekket i analysen av RTS artikkel 2. Det gjenstår dermed å se hva som vil skje med forslaget i høringsrunden, og hvor lang tid det vil ta før de nye forordningene blir vedtatt og gjennomført i norsk rett.

---

[188] SWD 2023/231 final, s. 24.

[189] NOU 1996:24 Betalingssystemer m.v. Utredning nr 3 fra Banklovkommisjonen, punkt 9.2.

[190] HR-2022-2468-A, avsnitt 20.

[191] Økokrim (2022) s. 49.

[192] COM 2023/367 final.

[193] I forslaget til ny ordlyd heter det at overvåkingen skal «enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services», jf. COM 2023/367 final, artikkel 83 (1)(c).

Til sist vil jeg rette bemerkninger til uklarheten tilknyttet rekkevidden av foretakenes plikt til å vurdere svindelraten etter RTS artikkel 18. Formålet med å vurdere svindelraten etter artikkel 18 er å gi anslag på hvor høy risiko det er for at en transaksjon er svindel. Ratene spesifiserer en terskel for hvilken svindelforekomst som overstiger lav risiko for svindel. Som kartlagt i analysen skal svindelraten både omfatte ikke godkjente betalingstransaksjoner og autorisert betalingssvindel.[194] Det kan argumenteres for at en sideeffekt av dette er at det etableres en forståelse av akseptert svindelrisiko i næringen. [195]

Svindelratene som fremgår av vedlegget til forordningen kan ansees som en spesifisert standard fra EUs side om hvilket risikonivå som kan tolereres innad i det europeiske markedet. Følgen av dette er at foretakenes vurdering av svindelraten skal fungere styrende for foretaket i etterlevelsen av de øvrige sikkerhetstiltakene i forordningen. Eksempelvis, dersom svindelraten i et foretak langt overstiger tersklene i vedlegget kan det gi indikasjon på at foretakets rutiner for overvåkingen etter artikkel 2 ikke er tilstrekkelige for å avdekke «uautoriserte og svigagtige betalingstransaktioner». At svindelraten kan – og bør, få denne virkningen, kunne kommet tydeligere til syne.

Håndtering av risiko tilknyttet egne produkter og tjenester er ikke noe nytt for foretak som tilbyr finansielle tjenester. Konvensjonelle banker tilbyr gjerne betalingstjenester i tillegg til tjenester som lån og kreditt, depositumkontoer og investeringsprodukter. Forutsetningsvis er konvensjonelle banker vant med å håndtere risiko, i form av kredittrisiko, likviditetsrisiko og renterisiko.[196] Som et utgangspunkt kan det dermed legges til grunn at betalingsforetak vurderer risiko tilknyttet deres virksomhet, og at denne risikovurderingen fungerer styrende for hvilke sikkerhetstiltak foretaket implementerer.

Den kan likevel stilles spørsmålstegn ved om svindelrisiko blir prioritert like høyt som eksempelvis kredittrisiko, likviditetsrisiko og renterisiko. Kredittrisiko, likviditetsrisiko og renterisiko, er typer av risiko som formodentlig vil oppleves som en eksistensiell risiko for konvensjonelle banker. Tilknyttet kredittrisiko, likviditetsrisiko og renterisiko er banken avhengig av å kunne levere kontrollerte risikoanalyser for å operere under nasjonale myndigheters tillatelse. Banker skal internt bestemme hvilken risiko foretaket kan tolerere, eksempelvis gjennom kredittkvalitetsnivåer, vurdering av total risiko konsentrert i en portefølje, store eksponeringer, likviditetsforhold og antallet finansielle kontrakter mulig utsatt for rentesjokk. Det er følgelig kategorier av risikoer som det kan antas at foretaket selv aktivt oppsøker.

---

[194] EBA- 2018-4032; EBA-2018-4034; EBA-2018-4044; EBA-2019-4702.

[195] Aven (2013) 462-468.

[196] Plikter til risikostyring av kredittrisiko, likviditetsrisiko og renterisiko følger av CRR og CRD IV, som gjennomfører Baselkomiteens anbefalinger om kapitalbufferkrav og pilar II. CRR/CRD IV er gjennomført i norsk rett i finansforetaksloven, finansforetaksforskriften og CRR/CRD-forskriften.

Svindelrisiko er til sammenligning en type risiko som uunngåelig kan antas å være til stede i bankens vanlige drift, og ansees dermed som en kilde til operasjonell risiko.[197] Når et foretak skal håndtere en operasjonell risiko vil det alminnelig sett bero på foretakets risikovurdering. For å måle om risikonivået i et foretak er innenfor akseptable grenser for å håndtere den operasjonelle risikoen vil foretak ofte anse det tilstrekkelig å sammenligne egen risiko opp mot konkurrenters risiko.[198] Kilden for foretaket til å vurdere forventet risiko for svindel beror i så måte i hovedsak på antallet reklamasjoner fra kunder, sett i sammenheng med hva som ansees som standarden i næringen. På dette grunnlag er det det nærliggende å anta at hva ulike betalingsforetak i sin interne drift anser som akseptabel risiko for svindel kan variere betydelig.[199]

Det kan ikke utelukkes at standarden lagt opp til av EBA i forordningen er et langt lavere risikonivå enn den som tidligere har vært akseptert som norm i næringen. Standarden fra EU er en kilde som burde veie betydelig tyngde enn vurdering av forventet svindelomfang på bakgrunn av hva som har vært norm i næringen tidligere.

4.6.2 Økonomiske insentiv til etterlevelse

(i) Offentligrettslig tilsyn og kontroll

Kravet til sterk kundeautentisering har vært i kraft i norsk rett siden 2019, og bestemmelsen som gjennomfører forordningen trådte i kraft i 2023. Per i dag har ikke Finanstilsynet publisert rapporter som viser tilsyn av foretakenes etterlevelse av kravet til sterk kundeautentisering. Det er følgelig uklart hvordan tilsynet konkret følger opp og vurderer etterlevelsen av overvåkingsforpliktelsene. Sett hen til at pliktene er relativt nye er det lite grunnlag for å vurdere om tilsynet er tilstrekkelig intensivt til å fungere som insentiv for etterlevelse.

(ii) Privatrettslig tapsrisiko – forholdet til tapsfordelingsreglene i fil. § 4-30

Tapsfordelingsreglene i fil. § 4-30 kommer etter sin ordlyd til anvendelse overfor «ikke godkjente betalingstransaksjoner».[200] Etter bestemmelsens første ledd har betalingstjenestetilbyder som utgangspunkt ansvar for kundens tap. Bakgrunnen for tapsfordelingsreglene er at tapsrisikoen skal insentivere foretakene til å investere i sikkerhetstiltak.[201] Som etterlevelsesrapporten til den europeiske kommisjonen gir uttrykk for har sikkerhetstiltakene i PSD 2 fått en svindelreduserende effekt overfor ikke godkjente betalingstransaksjoner. Det kan indikere at tapsfordelingsreglene har fått ønsket virkning som insentiv til etterlevelse.

---

[197] Se PSD 2 artikkel 95 (1); EBA/GL/2017/17, punkt 5.2 b); Basel (2001) s. 6.

[198] Gontarek, Bender (2019) s. 74-85.

[199] Levine, Ross (2004).

[200] Gjennomfører PSD 2 artikkel 71.

[201] Prop.92 LS (2019–2020) på s. 184 fl.

Som fremhevet ovenfor er det imidlertid en økende utfordring med autorisert betalingssvindel, hvor kunden er utsatt for sosial manipulering. Dette er transaksjoner som ansees godkjente etter finansavtaleloven, hvor tapsfordelingsreglene i fil. § 4-30 ikke kommer til anvendelse.

Uttalelser fra EBA i 2022 peker på at svindeltapet som følge av autorisert sosial manipuleringssvindel som oftest lempet over på kunden.[202] Samme tendens kan gjenfinnes i Norge.[203] Det at betalingstjenestetilbyder er tilnærmet sikret å få tapet erstattet av kunden på bakgrunn av tapsfordelingsreglene kan få den uheldige virkning at foretakene ikke er tilstrekkelig insentivert til å investere i overvåkingssystemer som egner seg til å avdekke betalingstransaksjoner godkjent av betaler som følge av sosial manipulering.

Til sammenligning kan det sees hen til standarden utarbeidet i Storbritannia om hvordan betalingstjenestetilbydere kan beskytte kunder mot autorisert betalingssvindel.[204] Standarden gjelder for privatkunder og små selskaper innen Storbritannia, og er frivillig å implementere. Standarden spesifiserer blant annet krav om tilbakeføring av kundens tap.

5 Transaksjonsovervåking etter hvitvaskingsloven med forskrift

5.1 Innledende bemerkninger

I dette kapittelet skal jeg se nærmere på transaksjonsovervåkningspliktene som gjelder for rapporteringspliktige etter hvitvaskingsloven med forskrift. Som nevnt innledningsvis avgrenser jeg til å vurdere pliktene relevante for rapporteringspliktige som operer som betalingsforetak, når foretaket gjennomfører fjernbetalingstransaksjoner.

Det rettslige utgangspunktet for transaksjonsovervåkingsplikten etter hvitvaskingsloven følger av § 24 (1), [205] hvor det heter at

> «[r]apporteringspliktige skal løpende følge opp kundeforhold. Oppfølgingen skal blant annet omfatte å overvåke at transaksjoner som utføres i kundeforholdet, er i samsvar med den rapporteringspliktiges innhentede opplysninger om kunden, kundens virksomhet og risikoprofil, midlenes opprinnelse og kundeforholdets formål og tilsiktede art».

[202] EBA/Op/2022/06, avsnitt 350-51.

[203] FinKN-2020-703; FinKN-2020-706; FinKN-2020-707; FinKN-2020-897; FinKN-2020-963.

[204] Lending Standards Board (2023). Contingent Reimbursement Model Code for APP scams (the CRM Code).

[205] Gjennomfører 4AMLD artikkel 13 (1)(d).

Det følger av ordlyden at transaksjonsovervåking inngår som del av den rapporteringspliktiges løpende oppfølgning av kunden. Forarbeidende til hvitvaskingsloven uttaler at formålet med den løpende oppfølgningen er «å oppdage avvikende atferd fra kunden». [206] Årsaken til dette er at avvikende adferd fra kunden kan vekke mistanke om hvitvasking eller terrorfinansiering. Overvåkingsplikten sikrer dermed at rapporteringspliktige følger med på kundens aktivitet,[207] slik at avvikende adferd – og dermed også mistanke om hvitvasking eller terrorfinansiering, blir kjent for foretaket.

I forarbeidene til hvvl. § 9 presiseres at utgangspunktet for å vurdere om det foreligger et avvik er den rapporteringspliktiges kunnskap om kunden.[208] Kunnskapen rapporteringspliktige har om kunden vil som oftest stamme fra gjennomførte kundetiltak etter hvitvaskingsloven kapittel 4. Kundetiltak er et begrep som brukes om innhenting av nærmere bestemte opplysninger om kunden. Formålet med kundetiltakene er at de rapporteringspliktige skal kjenne sine kunder (som et utslag av det såkalte «kjenn-din-kunde»-prinsippet), herunder hvem de er, det nærmere innholdet av kundeforholdet, hvilke tjenester og produkter de benytter hos den rapporteringspliktige, og omfanget av kundeforholdet, jf. hvvl. § 12.

Det følger av hvvl. § 24 (2) at der foretaket avdekker «tvil om tidligere innhentede opplysninger er tilstrekkelige eller korrekte» skal foretaket gjennomføre nye kundetiltak. Der foretaket kan konstatere at en handling representerer et avvik fra tidligere kjennskap om kunden og kundeforholdet skal foretaket gjennomføre nærmere undersøkelser, jf. hvvl. § 25. I tillegg presiserer hvvl. § 25 noen typer av mistenkelige transaksjoner som alltid skal underlegges nærmere undersøkelser. Det er innholdet og rekkevidden av kravene til å gjennomføre kundetiltak i den løpende oppfølgningen etter hvvl. § 24 og nærmere undersøkelser etter hvvl. § 25 jeg skal undersøke nærmere i det følgende.

For å gjøre dette vil jeg kartlegge formålet med overvåkingen (punkt 5.2), før jeg går over til å undersøke kravene nærmere. Sett hen til at grunnlaget for overvåkingen er opplysningene foretaket har om kunden vil jeg kartlegge hvilke opplysninger foretaket kan forventes å ha om kunden på bakgrunn av gjennomførte kundetiltak (punkt 5.3). Jeg vil ta utgangspunkt i plikten til å innhente kundeopplysninger ved etablering av kundeforhold, jf. hvvl. § 10 (1)(a). Som analysen vil avdekke er kundetiltakene i kundeetableringen grunnlaget for risikovurderingen av kunden. Risikovurderingen av kunden er styrende for intensiteten i oppfølgningen av kunden, deriblant transaksjonsovervåkingen.

[206] NOU 2016: 27 punkt 5.9.4.1.
[207] NOU 2016: 27 punkt 5.9.4.1.
[208] NOU 2016: 27 punkt 5.9.4.1.

Deretter vil jeg se nærmere på de konkrete kravene til overvåking som følger av hvvl. §§ 24 og 25 (punkt 5.4). I analysen avgrenser jeg til å vurdere overvåkingsforpliktelsene overfor kunder foretaket har etablert kundeforhold med. Avslutningsvis vil jeg vurdere i hvilken grad pliktene til overvåking i hvitvaskingsloven er egnet til å oppfylle sine formål (punkt 5.5).

5.2 Formål: Avdekke mistenkelige transaksjoner for å *avdekke* hvitvasking og terrorfinansiering

Formålet med hvitvaskingsloven er «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. hvvl. § 1 (1).[209] I hvvl. § 1 (2) presiseres videre at

> «[t]iltakene i loven skal beskytte det finansielle og økonomiske systemet samt samfunnet som helhet ved å forebygge og avdekke at rapporteringspliktige brukes eller forsøkes brukt som ledd i hvitvasking eller terrorfinansiering».

Det følger av formålsbeskrivelsen at bakgrunnen for hvitvaskingsloven er å forhindre at den finansielle sektors integritet, stabilitet og omdømme blir skadet som følge av hvitvasking og terrorfinansiering.[210] I tillegg til å sikre stabilitet og tillit i finanssystemet har loven også som formål å beskytte økonomien og samfunnet som sådan mot skadevirkningene av hvitvasking og terrorfinansiering.

Hvitvasking og terrorfinansiering kan skade det indre markedet og internasjonal utvikling, noe som anerkjennes som et så omfattende problem at det må adresseres på EU-nivå.[211] Som fremhevet i forarbeidene til hvitvaskingsloven er det derfor også et formål med loven å forebygge primærlovbruddet som ligger til grunn for den profittmotiverte kriminaliteten.[212] Hensikten er å skape vekselvirkning mellom kriminalisering av hvitvasking og effektiv bekjempelse av den profittmotiverte kriminaliteten som ligger til grunn for hvitvaskingen. Forutsetningen for at noe faller inn under betegnelsen hvitvasking er nettopp at det er begått et primærlovbrudd som har frembrakt et utbytte av økonomisk verdi.[213] Dersom det er vanskelig å hvitvaske utbyttet, vil det forutsetningsvis være mindre attraktivt å begå primærlovbruddet.[214]

---

[209] Gjennomfører 4AMLD artikkel 1 (1).

[210] 4AMLD, fortalen avsnitt 2.

[211] 4AMLD, fortalen avsnitt 1.

[212] NOU 2016: 27 s. 22.

[213] Se strl. §§ 332 og 337.

[214] Se NOU 2002: 4 Ny straffelov Straffelovkommisjonens delutredning VII, hvor det i punkt 9.7. uttales at «(h)ovedformålet med bestemmelsen om heleri og hvitvasking er å forebygge slike vinningsovertredelser, ved å gjøre det vanskeligere for gjerningspersonen å få glede av utbyttet».

Overvåking av transaksjoner er helt sentral for å oppfylle formålet om å *avdekke* hvitvasking og terrorfinansiering, jf. hvvl. § 1 (1). Overvåkingen gjør det nettopp *mulig* å avdekke hvitvaskingstransaksjonen. Hvitvasking er i sin kjerne utnyttelse av det finansielle systemet, og innebærer å skjule kriminelt utbytte i den legitime pengestrømmen. Det er avgjørende at foretak som gjennomfører betalingstransaksjoner har mekanismer på plass for å avdekke mistanke om at en transaksjon i realiteten er utbytte fra kriminelle handlinger.

Risikotilnærmingen gjennomsyrer hvordan pliktene til rapporteringspliktige er formulert i hvitvaskingsloven. Risiko er i seg selv en term med et lite avklart og ensartet innhold. I juridiske sammenhenger beskrives risiko ofte som et produkt av sannsynlighet og konsekvens.[215] I hvitvaskingsloven har imidlertid risiko blitt tillagt et mer presist innhold. Som det følger av anbefalingene til FATF, som ligger til grunn for hvitvaskingsloven, er risiko et resultat av usikkerhet knyttet til om målet med loven vil lykkes.[216] Sagt på en annen måte anvendes en risikobasert tilnærming til måloppnåelse. Virkningen av den risikobaserte tilnærmingen er at den rapporteringspliktige kan bruke mindre ressurser der det er lav risiko, og motsetningsvis skal bruke mer ressurser der det er høyere risiko.[217]

5.3 Plikt til å gjennomføre kundetiltak i etableringen av kundeforhold etter hvvl. § 12, jf. § 10

5.3.1 Rettslig utgangspunkt

Problemstillingen jeg skal undersøke i det følgende er hvilke opplysninger foretaket kan forventes å ha om kunden. Jeg vil som nevnt ta utgangspunkt i plikten til å gjennomføre kundetiltak «ved etablering av kundeforhold», jf. hvvl. § § 10 (1).

Det første spørsmålet er når kundeforholdet etableres. Tidspunktet for når et kundeforhold ansees som etablert er presisert i hvitvaskingsforskriften § 4-1 (1) hvor det heter at kundeforhold etableres «når kunden kan bruke den rapporteringspliktiges tjenester». Ytelse av betalingstjenester er et klassisk eksempel på tjenester som etablerer kundeforhold.[218] Som fremhevet av departementet i hvitvaskingslovens forarbeider vil enhver kontakt med kunden for mange rapporteringspliktige innebære «etablering av kundeforhold», for eksempel ved åpning av konto

[215] Til illustrasjon brukes tilsvarende risikobegrep på flere områder i finansmarkedsretten, som ISO 31000:2018, Risk management – Guidelines; ISO 37001:2016, Anti-bribery management systems – Requirements with guidance for use; ISO/TR 31004:2013, Risk management – Guidance for the implementation of ISO 31000; SN-ISO Guide 73:2009, Risk management – Terminology; ISO 31010:2009, Risk management – Risk assessment techniques.

[216] FATF (2010) s. 13.

[217] NOU 2016: 27 s. 62 fl.

[218] Hvitvaskingsforskriften § 4-1; RFT-2022-4 s. 21.

eller utføring av et oppdrag.[219] En enkeltstående transaksjon kan følgelig også etablere kundeforhold.

Det neste spørsmålet er hvordan kundeforholdet etableres. Det følger av hvvl. § 12 at kundeforhold som utgangspunkt etableres med «personlig fremmøte», jf. forutsetningen i hvvl. § 12 (2) om hvordan kundens identitet kan bekreftes. Kundeforhold kan også på visse vilkår etableres uten personlig fremmøte.[220] Der kundeforhold etableres uten personlig fremmøte kan kundens identitet bekreftes med en eID, jf. hvitvaskingsforskriften § 4-3 (4). I praksis etableres de fleste nye kundeforhold i Norge uten personlig fremmøte ved bruk av BankID.

Innholdet i kundetiltakene ved kundeetablering når kunden er en fysisk person følger av hvitvaskingsloven § 12. Det følger av § 12 (1) at foretaket skal innhente personopplysninger som navn, fødselsnummer eller tilsvarende, og adresse. I tillegg skal foretaket avgjøre om det finnes en reell rettighetshaver i tillegg til kunden, jf. § 12 (3), og vurdere om kunden er en politisk eksponert person («PEP»), jf. § 12 (4). Til sist skal foretaket «innhente og vurdere nødvendige opplysninger om kundeforholdets formål og tilsiktede art», jf. § 12 (5).

I det følgende vil jeg si noe mer om innholdet i plikten til å «innhente og vurdere nødvendige opplysninger om kundeforholdets formål og tilsiktede art» etter hvvl. § 12 (5). Som den videre analysen vil avdekke avhenger rekkevidden av plikten av foretakets risikovurdering av kunden. Jeg vil av den grunn også i det følgende se nærmere på plikten til å risikovurdere kunden i forbindelse med kundeetableringen.

5.3.2 Plikten til å *innhente* «nødvendige opplysninger om kundeforholdets formål og tilsiktede art»

Plikten til å «*innhente og vurdere* nødvendige opplysninger om kundeforholdets formål og tilsiktede art» (min kursivering) i hvvl. § 12 (5) reiser noen tolkningsspørsmål. For det første hvilke opplysninger som må *innhentes*. For det andre hva som kreves av foretakets *vurdering* av innhentede opplysninger.

Jeg vil først se nærmere på hvilke opplysninger foretaket må innhente. Ordlyden «nødvendige opplysninger om kundeforholdets formål og tilsiktede art» gir i seg selv liten veiledning om hvilke opplysninger foretaket skal innhente. I forarbeidene til hvitvaskingsloven gir hvitvaskingsutvalget imidlertid en liste over opplysninger som kan innhentes for å klarlegge kundeforholdets formål og tilsiktede art, herunder «opplysninger om hensikten eller bakgrunnen for kun-

[219] NOU 2016: 27 s. 224.

[220] Jeg vil behandle de nærmere vilkårene for dette i neste punkt.

deforholdet eller transaksjonen, midlenes opprinnelse, hvem kunden skal handle med og forventet transaksjonsmønster, herunder typer transaksjoner, transaksjonshyppighet og –størrelse».[221]

Det reiser et spørsmål om foretaket må innhente alle disse opplysningene om alle kundene i forbindelse med kundeetableringer. Det følger av ordlyden i hvvl. § 12 (5) at opplysningene må være «nødvendige». Det innebærer at omfanget av opplysninger kan avpasses ved behov. At rekkevidden av opplysninger vil kunne variere fra kunde til kunde er videre lagt til grunn i lovens forarbeider. Flertallet i hvitvaskingsutvalget uttaler eksempelvis at «[v]ed kjøp av varer vil formålet ofte gi seg selv på bakgrunn av varen som handles».[222] I tråd med dette uttales det i proposisjonen at «[i] en del kundeforhold vil det være selvforklarende hva som er formålet, slik at det ikke vil være «nødvendig» å innhente ytterligere opplysninger».[223] Det sentrale er følgelig at rapporteringspliktige har en formening om hvorfor kundeforholdet etableres og hva det skal brukes til. Listen i forarbeidene over opplysninger som kan innhentes kan dermed forstås som en veiledende liste.

Det følger videre av hvvl. §§ 16 og 17 at foretaket kan avpasse informasjonsinnhentingen ytterligere, dersom kunden underlegges henholdsvis forenklede eller forsterkede kundetiltak. Etter hvvl. § 16 «kan» foretaket gjennomføre forenklede kundetiltak overfor kunder med «lav risiko for hvitvasking eller terrorfinansiering». Etter hvvl. § 16 innebærer forenklede kundetiltak at kravet i hvvl. § 12 (5) til å innhente og vurdere nødvendige opplysninger om kundeforholdets formål og tilsiktede art «lempes». Ordlyden «lempes» kan gi antydninger om at foretaket kan se bort fra kravet om å «innhente nødvendige opplysninger om kundeforholdets formål og tilsiktede art» etter hvvl. § 12 (5). Det følger imidlertid av forarbeidene til bestemmelsen at dette ikke er tilfelle.

Med henvisning til FATF sin forklarende note 21 til anbefaling 10 fremgår det av hvitvaskingsutvalget at den rapporteringspliktige i stedet for å be kunden oppgi kundeforholdets formål og tilsiktede art, kan foretaket innhente informasjonen basert på typen transaksjoner som gjennomføres eller kundeforhold som etableres.[224] Uttalelsen er gjengitt i proposisjonen.[225] Foretaket er følgelig fremdeles forpliktet til å gjøre seg opp en formening om kundeforholdets formål og tilsiktede art, men behøver ikke å innhente disse opplysningene direkte fra kunden.

[221] NOU 2016: 27 punkt 5.2.4.9.
[222] NOU 2017: 27 punkt 5.2.4.9.
[223] Prop.40 L (2017–2018) s. 174.
[224] NOU 2016: 27 punkt 5.3.3.
[225] Prop.40 L (2017–2018) s. 80.

Det neste spørsmålet er betydningen av at kunden underlegges såkalte forsterkede kundetiltak. Det følger av hvvl. § 17 at for kundene klassifisert som «høy risiko for hvitvasking eller terrorfinansiering» skal rapporteringspliktige gjennomføre forsterkede kundetiltak, jf. hvvl. § 17. Etter § 17 innebærer det at rapporteringspliktige «må iverksette ytterligere nødvendige tiltak for å sikre kjennskap om kunden, reelle rettighetshavere og kundeforholdets formål og tilsiktede art». Det følger av dette at foretakets plikter overfor høyrisikokunder er langt mer omfattende enn overfor lavrisikokunder.[226]

Som redegjørelsen ovenfor illustrerer opererer hvitvaskingsloven forutsetningsvis med tre risikoprofiler; «høy»,[227] «lav»,[228] og en restkategori som kan omtales som normal risiko. Adgangen til å gjøre forenklede kundetiltak overfor lavrisikokunder og plikten til å gjøre forsterkede kundetiltak overfor høyrisikokunder viser at omfanget av opplysninger det er «nødvendig» å innhente om kunden og kundeforholdet etter hvvl. § 12 (5) avpasses etter kundens risikoprofil. Konsekvensen av dette er at mengden opplysninger foretaket har om de ulike kundene vil variere. For å kartlegge hvilke opplysninger foretaket kan forventes å ha om kundene er det relevant å se nærmere på pliktene til å vurdere kunderisikoen.

(i) Plikt til å vurdere kunderisikoen

Foretakets plikt til å vurdere risiko følger av hvvl. § 7. Det heter i bestemmelsens annet ledd at foretaket skal ta i betraktning risiko knyttet til (a) foretakets egen virksomhet, (b) produkter, tjenester og kundeforhold, (c) type kunder, kundegrupper og geografiske forhold. Disse tre risikokategoriene i hvvl. § 7 (2) sikrer at foretaket identifiserer sårbarheter i virksomheten for å bli utnyttet til hvitvasking eller terrorfinansiering.

Hvilke momenter ved kunden og virksomheten som kan tilsi at det er sårbarheter ved virksomheten er spesifisert i hvitvaskingsforskriften. Etter forskriften § 4-9 er momenter som kan tilsi høy risiko knyttet til *kunden* dersom det er uvanlige omstendigheter knyttet til kundeforholdet, kunden er bosatt i områder som ansees å innebære høyere risiko, visse typer juridiske personer, arrangementer og selskapsstrukturer, samt kontantbaserte virksomheter.[229] Momenter som kan tilsi høy risiko knyttet til typen *produkt eller tjeneste* er om transaksjonen, tjenesteytelse eller leveringskanal er «private banking», om produkter og tjenester fremmer anonymitet, dersom etablering av kundeforhold eller transaksjoner skjer uten personlig fremmøte og uten bruk av

[226] Hvitvaskingsforskriften § 4-10 presiserer hvordan forsterkede kundetiltak skal gjennomføres overfor kundeforhold og transaksjoner med tilknytning til høyrisikoland.

[227] Hvvl. § 17.

[228] Hvvl. § 16.

[229] Hvitvaskingsforskriften § 4-9 (a).

elektronisk signatur, betalinger fra ukjente tredjeparter, samt nye produkter og tjenester.[230] *Geografiske risikomenter* er kundeforhold med tilknytning til land uten tilfredsstillende og effektive tiltak for å bekjempe hvitvasking, land med betydelig korrupsjon og annen kriminalitet, land underlagt sanksjoner og land som finansierer eller støtter terrorvirksomhet.[231]

Som listen over risikomomenter illustrerer, skal rapporteringspliktige gjøre en bred og helhetlig vurdering av både kunderisikoen og sårbarheter ved virksomheten. Risikoklassifiseringen av kunden er resultat av denne helhetsvurderingen. Det innebærer at dersom kunden får risikoutslag på en av faktorene opplistet i hvitvaskingsloven § 7, vil ikke det nødvendigvis innebære at kunden skal plasseres i en høyrisikokategori.

(ii) Kundeetablering med eID – betydningen for kunderisikovurderingen
Jeg vil i det følgende knytte noen særlige bemerkninger til risikomomentet som knytter seg til om «kundeforhold eller transaksjoner som opprettes og utføres uten personlig oppmøte, uten at tiltak som elektronisk signatur benyttes», jf. hvitvaskingsforskriften § 4-9. Jeg vil ta utgangspunkt i kundeetablering med BankID, siden den er den mest utbredte løsningen for elektroniske signaturer på det norske markedet.

Årsaken til at jeg vil se nærmere på kundeetablering med BankID er at BankID har flere bruksområder med betydning for foretakets forpliktelser i forbindelse med gjennomføring av betalingstransaksjoner. BankID kan som nevnt innledningsvis i kapittelet brukes til å etablere kundeforhold med rapporteringspliktige. Gjennomføring av en enkeltstående betalingstransaksjon kan også etablere kundeforhold. Der BankID brukes til å gjennomføre en betalingstransaksjon vil løsningen dermed fungere både som betalingsinstrument og som sterk kundeautentisering, jf. punkt 2.3, i tillegg til at transaksjonen kan etablere kundeforhold. Det illustrerer betydningen av BankID på det norske markedet.

BankID er imidlertid også sårbar for å bli misbrukt. I fastleggelsen av foretakets plikt til å vurdere kundens risiko når BankID er involvert i kundeetablering finner jeg det følgelig relevant å se nærmere på betydningen av at en eID, som for alle praktiske formål betyr BankID, benyttes som kundeidentifikasjon for foretakets vurdering av kunderisikoen.

Årsaken til at kundeidentifikasjon utgjør et viktig element i risikovurderingen er at foretaket er avhengig av å sikre at transaksjoner skjer ut fra legitime kontoer. Dette kan illustreres med rapporteringspliktiges plikt til å avklare i hvilken grad det er en «reell rettighetshaver» i tillegg

[230] Hvitvaskingsforskriften § 4-9 (b).
[231] Hvitvaskingsforskriften § 4-9 (c).

til kunden tilknyttet kundeforholdet, jf. hvitvaskingsloven § 12 (3). I hvitvaskingsloven defineres «reell rettighetshaver» som en fysisk person som «i siste instans eier eller kontrollerer kunden, eller som en transaksjon eller aktivitet gjennomføres på vegne av», jf. hvvl. § 2 (e). Formålet med å være kjent med kundeforholdets reelle rettighetshavere er blant annet at foretaket skal kunne kontrollere midlenes opprinnelse.[232]

Som plikten til å avgjøre reelle rettighetshavere illustrerer er hvitvaskingslovens plikter bygget på forutsetningen om at foretaket vet hvem som bruker og kontrollerer kundeforholdet. Dersom kontoetableringen ikke er legitim, vil virksomheten ikke foreta en korrekt risikoklassifisering av kunden. Da vil det være mye vanskeligere for banken å undersøke midlenes opprinnelse, og avdekke om midler i kundeforholdet har tilknytning til hvitvasking eller terrorfinansiering, jf. hvitvaskingsloven § 25.

Det rettslige grunnlaget for kundeidentifikasjon følger av hvitvaskingsloven § 12 (2) som fastsetter at kundens identitet som utgangspunkt skal «bekreftes ved personlig fremmøte». I ordlyden «bekreftelse ved personlig oppmøte» ligger det at en kundebehandler møter kunden fysisk og kontrollerer at de innhentede opplysningene tilhører vedkommende. For eksempel at kunden drar til bankens filial for å gjennomføre identitetskontroll av kundens identifikasjonsdokumenter.

Det er imidlertid gjort unntak fra kravet om «personlig fremmøte» i hvvl. § 12 (2) annet punktum. Det kan eksempelvis være dersom kunden i stedet etablerer kundeforholdet via nettbanken eller over telefon. For at unntaket fra personlig fremmøte kan anvendes oppstiller § 12 krav om at kundens identitet bekreftes med «ytterligere dokumentasjon» eller at det gjennomføres «ytterligere tiltak». I forarbeidene er videosamtale gitt som eksempel på tiltak som vil oppfylle lovens krav til supplerende tiltak.[233]

Årsaken til at det som utgangspunkt kreves supplerende tiltak ved legitimasjon uten personlig fremmøte er fordi «non-face-to-face»-kunderelasjoner etter det fjerde hvitvaskingsdirektivets Annex II er ansett som et forhold med høyere risiko for at kundeforholdet vil bli brukt til hvitvasking og terrorfinansiering.[234] Kundeforhold med potensielt høyere risiko for hvitvasking og terrorfinansiering nødvendiggjør etter denne risikovurderingen iverksettelse av supplerende tiltak for å sikre kjennskap til kunden.[235]

---

[232] Hvvl. § 18 (2)(b); Rui (2012) side 283-284.

[233] NOU 2016: 27 s. 79.

[234] Se også EBA/GL/2021/02 punkt 4.31.

[235] Hvvl. § 17.

Det følger imidlertid av hvitvaskingsforskriften § 4-3 fjerde ledd at «[e]lektronisk signatur er gyldig legitimasjon for fysisk person når identiteten ikke skal bekreftes ved personlig fremmøte». Vilkåret for at elektronisk signatur kan brukes som gyldig legitimasjon uten fysisk oppmøte er at den elektroniske signaturen tilfredsstiller kravene til eID-ordning i selvdeklarasjonsforskriften § 3 og er oppført på publisert liste i henhold til § 13 første ledd i nevnte forskrift. Det følger av sammenhengen mellom hvitvaskingsforskriften § 4-3 fjerde ledd og selvdeklarasjonsforskriften § 3 at eID på sikkerhetsnivå 'høyt' er tilstrekkelig legitimasjon av kunden, og likestilles med identitetskontroll ved «personlig fremmøte». Det er også lagt til grunn i finanstilsynets rundskriv.[236]

eID på høyt sikkerhetsnivå fungerer dermed både som signeringsverktøy og som et gyldig legitimasjonsdokument ved etablering av kundeforhold. Det muliggjør å etablere kundeforhold via bankens hjemmesider på internett, uten at kunden fysisk må oppsøke bankens filial for å gjennomføre identitetskontrollen eller at det gjennomføres supplerende tiltak.

Unntaket for supplerende tiltak etter hvitvaskingsforskriften § 4-3 svarer til modifiseringene gjort av EU i det femte hvitvaskingsdirektivet, som åpner for å bruke eID-ordninger som oppfyller kravene i eIDAS-forordningen[237] til å legitimere seg elektronisk.[238] Ved å tillate elektronisk identifikasjon i tråd med eIDAS-forordningen som bekreftelse på identitet etter hvitvaskingsreglementet samordnes det fjerde hvitvaskingsdirektivet og eIDAS-forordningen.

Integreringen av eIDAS og det femte hvitvaskingsdirektivet er i tråd med anbefaling fra FATF fra 2020 i deres veiledningsrapport om digitale identiteter.[239] Etter modifikasjonen i det femte hvitvaskingsdirektivet vil «non-face-to-face»-kundeforhold bekreftet med eID ikke lenger være en faktor som tilsier høy risiko.[240] Unntaket for krav til supplerende tiltak der identiteten til kunden bekreftes med eID gir uttrykk for en endret holdning til den risiko «anonyme» kundeforhold representerer for hvitvasking.

FATF fremhever at mange eID-systemer overholder høye teknologiske, organisatoriske og styringsstandarder.[241] Systemene har potensiale til å forbedre påliteligheten, sikkerheten, personvernet og bekvemmeligheten for fysiske personer til å identifisere seg i en rekke settinger. I

---

[236] RTF-2019-8 kap. 4.3.1.2.

[237] Europaparlamentets rådsdirektiv (EU) No 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS).

[238] 5AMLD artikkel 13.

[239] FATF (2020a) avsnitt 3, 74 og 87-89.

[240] 5AMLD, Annex III.

[241] FATF (2020a) avsnitt 33.

tillegg er eID-systemer effektive og kostnadseffektive, og muliggjør økt inkludering av tilgang på banktjenester ved å gjøre det mulig å bevise offisiell identitet på flere måter.[242]

Forutsetningen som oppstilles av FATF, for at bruk av eID til å bekrefte kundens identitet er et lavrisikomoment, er at eID-systemet er «reliable» (pålitelig), «independent» (uavhengig), og at det er på plass «appropriate risk mitigation measures» (hensiktsmessige sikkerhetsmekanismer).[243] EU har bestemt at eID-ordninger på høyt sikkerhetsnivå etter eIDAS er tilstrekkelig sikre til å kunne likestilles med personlig fremmøte.[244]

Det kan stilles spørsmål om det i noen tilfeller allikevel kan kreves at foretaket gjør supplerende tiltak når eID på høyt sikkerhetsnivå brukes til kundeidentifikasjon ved etablering av kundeforhold. FATF understreker i sine anbefalinger at selv om eID-en er godtatt av nasjonal myndighet som kundetiltak, og må ansees som et pålitelig og uavhengig system, kan det i noen tilfeller være krav til ytterligere sikkerhetstiltak.[245] Det samme er lagt til grunn i norsk rett.

Som det følger av rundskrivet til hvitvaskingsloven er det nødvendig med en «risikobasert tilnærming» for å avgjøre om det allikevel er behov for supplerende tiltak, der kundeforholdet etableres uten personlig fremmøte.[246] Det gis ingen retningslinjer i rundskrivet for den risikobaserte tilnærmingen. Det er allikevel nærliggende å forstå henvisningen til en risikobasert tilnærming som en anvisning på risikovurderingen som finansinstitusjonen for øvrig er forpliktet til i henhold til hvvl. §§ 7 og 9.

Viktigheten av at foretaket overholder de øvrige kravene til risikovurderinger blir også understreket av FATF i relasjon til bruk av eID-systemer for identitetsbekreftelse. Om eID-systemer som oppfyller eIDAS-forordningen uttaler FATF spesifikt i Appendix E at bruken av eID særlig nødvendiggjør «management and organisation» av finansinstitusjonen, og peker på behovet for å ha på plass nødvendige risikovurderinger av kunden og risikohåndtering av egen virksomhet.[247] For overholdelse av tilstrekkelig «management and organisation» av finansinstitusjonen ved bruk av eID fremhever FATF at det er særlig viktig at finansinstitusjoner overholder kravene til kundetiltak.[248] Ved inngåelse av kundeforhold står plikten til å vurdere risikoen som

[242] FATF (2020a) avsnitt 35 og 36.
[243] FATF (2020a) avsnitt 171.
[244] FATF (2020a) avsnitt 141 og 156.
[245] FATF (2020a), se figur på side 48.
[246] RFT-2022-4 s. 30.
[247] FATF (2020a) avsnitt 171 og Appendix E
[248] FATF (2020a) avsnitt 89.

kommer til uttrykk gjennom de innhentede opplysningene om kunden og kundeforholdet sentralt. Med det går jeg over til neste punkt, hvor jeg vil se nærmere på plikten til å «vurdere» innhentede opplysninger, jf. hvvl. § 12 (5).

5.3.3 Plikt til å *vurdere* «nødvendige opplysninger om kundeforholdets formål og tilsiktede art»

Det følger av en naturlig språklig forståelse av ordlyden «vurdere» at foretaket må gjøre seg opp en mening om hvorfor kundeforholdet er etablert og hva kundeforholdet skal brukes til. Det er følgelig ikke tilstrekkelig at foretaket innhenter denne typen informasjon. Den rapporteringspliktige må også ta stilling til opplysningene kunden oppgir.

Det at foretaket må ta stilling til opplysningene kunden oppgir reiser et tolkningsspørsmål om hvilken vurdering den rapporteringspliktige skal foreta og hva som er konsekvensen av vurderingen foretatt av foretaket. En vurdering foretaket er forpliktet til å gjøre er regulert i hvitvaskingsloven § 21. Det følger av hvvl. § 21 (1) at dersom kundetiltak ikke kan gjennomføres «skal rapporteringspliktige ikke etablere kundeforholdet eller utføre transaksjonen». Det følger av en naturlig forståelse av ordlyden at dersom foretaket ikke får gjennomført informasjonsinnhentingen på tilfredsstillende måte skal foretaket avstå fra å etablere kundeforholdet. Det følger av dette at rapporteringspliktige må vurdere hvorvidt kundeforholdet i det hele tatt skal etableres. Det reiser et spørsmål om hvilke forhold som enten skal eller kan vektlegges for å avgjøre om kundetiltaket er gjennomført på tilfredsstillende måte.

Ordlyden i hvvl. § 21 (1) annet punktum kan gi en pekepinn. Det følger av bestemmelsen at rapporteringspliktige på bakgrunn av vurderingen om kundetiltakene er gjennomført skal «vurdere om det er grunnlag for nærmere undersøkelser og rapportering i samsvar med §§ 25 og 26». Pliktene til å gjennomføre nærmere undersøkelser og rapportering i hvvl. §§ 25 og 26 utløses begge ved mistanke om hvitvasking eller terrorfinansiering.[249] Av denne sammenhengen kan man trekke slutningen at kundetiltak ikke er gjennomført på en tilfredsstillende måte dersom de ikke er egnet til å forsikre den rapporteringspliktige om at kundeforholdet vil benyttes til legitime formål. Denne tolkningen samsvarer med at hvitvaskingsloven overordnet har til formål å forebygge hvitvasking og terrorfinansiering, jf. hvvl. § 1.

Et videre spørsmål er hvilke forhold som kan tilsi at kundeforholdet kan forsøkes benyttet til illegitime formål. Det finnes kun et fåtall av eksempler fra praksis hvor spørsmål om avslag på henvendelser om kundeetablering har kommet på spissen. Av den praksisen som finnes har

[249] Nærmere om mistanketerskelen i del III.

avslagsgrunner blant annet vært alvorligheten i kundens tidligere straffedomfellelser,[250] og tilknytning til kriminell virksomhet.[251]

Til sammenligning er det langt mer praksis tilknyttet oppsigelse av kundeforhold. Etter hvvl. § 24 (4) skal kundeforholdet avsluttes dersom kundetiltak ikke lar seg gjennomføre på tilfredsstillende måte. Selv om praksisen knyttet til oppsigelse av kundeforhold ikke er direkte overførbar, kan den allikevel gi en pekepinn på hvilke momenter rapporteringspliktige kan legge vekt på i vurderingen av om kundetiltaket er tilfredsstillende gjennomført. Et slikt eksempel er FinKN-2018-489, som gjaldt oppsigelse av kundeforhold etter fil. 1999 § 14.[252]

I saken for Finansklagenemnda hadde kundeforholdet blitt avsluttet fordi dokumentasjonen kunden fremla til banken i forbindelse med gjennomføringen av kundetiltak fremsto som egenprodusert og uten slik dokumentasjonsverdi som banken trenger for å kunne gjennomføre kundekontroll etter hvitvaskingsloven. Banken fikk derfor medhold i oppsigelsen av kundeforholdet. Dersom man overfører uttalelsen til tilfeller som gjelder etablering av kundeforhold, kan uttalelsen gi uttrykk for at banken i gjennomføring av kundetiltakene må påse at dokumentasjonen og informasjonen kunden fremlegger i forbindelse med kundeetableringer er ekte og troverdige.[253]

Det inngår i dette at foretaket skal vurdere om de innhentede opplysningene er troverdige og ikke fabrikkerte eller falske. Det at opplysningene som oppgis må være troverdige vil fungere som en sikkerhet for at kunden er den de utgir seg for å være, og at kunden har legitime hensikter med kundeforholdet.[254]

I den forbindelse reiser det seg et spørsmål om hvordan et kundeforhold etablert med BankID uten supplerende vil bli risikoklassifisert. BankID er selvdeklarert som eID-ordning på høyeste sikkerhetsnivå,[255] og brukes som nevnt ovenfor i praksis til å etablere kundeforhold uten per-

---

[250] FinKN-2020-973, hvor kunden hadde vært tiltalt og senere frifunnet for innenlands terrortrussel.

[251] LB-2023-32107 (Borgarting), som gjaldt spørsmål om et forsikringsselskap kunne nekte fornyelse av skadeforsikringen for to kunder grunnet deres tilknytning til motorsykkelklubben Hells Angels.

[252] Erstattet i ny lov av fil. § 4-43.

[253] Se også EBA/GL/2022/15, punkt 4.3.

[254] For nærmere drøftelse av skjæringspunktet for når foretakets vurdering av kundeopplysninger utløser avvisningsplikt, se Rui (2023) s. 2–49.

[255] BankID er notert som sikkerhetsnivå 'høyt' av EU, jf. EU (2023). Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (2023/C 237/06). Official Journal of the European Union, C 237/6; Se også uttalelse fra den europeiske kommisjonen i Opinion No. 3/2022.

sonlig fremmøte. På bakgrunn av hvitvaskingsforskriften § 4-3, sett i sammenheng mmed rettsutviklingen i EU, er det nærliggende å anta at foretak basert på BankIDs sikkerhetsklassifisering vil anse kundeetablering med BankID som et moment som taler for lav risiko for hvitvasking og terrorfinansiering tilknyttet kunden.[256] Årsaken til dette er at identiteten til kunden formodentlig er blitt bekreftet på en sikker måte, noe som skal indikere at rapporteringspliktige med stor sikkerhet vet hvem som etablerer kundeforholdet. Bruken av BankID gjør det som presumtivt troverdig at kundeetableringen er legitim.

Om kundeetableringen gjelder grunnleggende banktjenester, som bankkonto, debetkort og tilgang på nettbank,[257] vil det også være en type tjeneste hvor det generelt sett antas å være lav risiko for hvitvasking og terrorfinansiering.[258] Følgelig er det grunn til å tro at kundeetablering om grunnleggende banktjenester med BankID er et moment som taler for at det er lav risiko for hvitvasking tilknyttet kundeforholdet.

Sett hen til at risikovurderingen etter hvitvaskingsloven er en finmasket vurdering, sammensatt av en kompleks, sammensatt og skjønnsmessig vurdering, er det vanskelig å si noe konkret om hvordan en kunde som etablerer kundeforhold med BankID typisk vil bli risikoklassifisert. Men, med mindre det er andre opplysninger om kunden, som opplysninger om midlenes opprinnelse, hvem kunden skal handle med og forventet transaksjonsmønster, herunder typer transaksjoner, transaksjonshyppighet og –størrelse, som tilsier at det vil være risiko for hvitvasking eller terrorfinansiering tilknyttet kundeforholdet, er det allikevel grunn til å tro at kundeetableringer med BankID ofte vil klassifiseres som lav risiko. Da er det også nærliggende å anta at den rapporteringspliktige vil benytte seg av adgangen til å underlegge kunden forenklede kundetiltak, jf. hvvl. § 16.

5.4 Plikt til å overvåke at transaksjoner som utføres i kundeforholdet er i samsvar med innhentede opplysninger om kundeforholdet

5.4.1 Rettslig utgangspunkt – plikt til løpende oppfølgning, jf. hvvl. § 24, og iverksettelse av nærmere undersøkelser, jf. hvvl. § 25

Nå som det er fastlagt hvilke opplysninger det kan forventes at foretaket har om kundene, går jeg over til å vurdere plikten til å overvåke at kundens handlinger samsvarer med opplysningene om kunden. Det rettslige utgangspunktet for plikten til å overvåke kundens transaksjoner er hvvl. § 24 (1), som oppstiller plikt til «å overvåke at transaksjoner som utføres i kundeforholdet, er i samsvar med den rapporteringspliktiges innhentede opplysninger om kunden». Det følger

[256] 5AMLD Annex III.

[257] RFT-2022-4, punkt 4.3.1.5.

[258] Hvitvaskingsforskriften § 4-6 annet ledd punkt 4.

av bestemmelsens annet ledd at kundetiltak alltid skal gjennomføres ved «tvil om tidligere innhentede opplysninger er korrekte eller tilstrekkelige». Det følger av sammenhengen at dersom en transaksjon eller et transaksjonsmønster er egnet til å skape slik «tvil» skal foretaket iverksette kundetiltak overfor kunden. Det springende punktet er dermed hva som skal til for at det foreligger «tvil om tidligere innhentede opplysninger er korrekte eller tilstrekkelige».

Ordlyden «tvil» oppstiller en lav terskel, og trekker i retning av at det er tilstrekkelig med usikkerhet. Det følger av dette at i den grad en transaksjon eller et transaksjonsmønster representerer en endring i kundeadferd fra innhentede opplysninger om midlenes opprinnelse, hvem kunden skal handle med og forventet transaksjonsmønster, herunder typer transaksjoner, transaksjonshyppighet og –størrelse,[259] skal foretaket iverksette kundetiltak. Sett hen til den lave terskelen for å iverksette kundetiltak trekker det i retning av at en transaksjon eller et transaksjonsmønster ikke behøver å være en betydelig eller markant endring i kundeadferd for å utløse kundetiltak. Det innebærer at transaksjonsovervåkingen må være så treffsikker at den også avdekker mindre endringer.

Basert på denne analysen er det grunn til å forvente at transaksjonsovervåkingen eksempelvis avdekker at en kunde som har oppgitt at vedkommende kun vil gjennomføre innenlandstransaksjoner, gjennomfører en transaksjon til utlandet. Et annet tenkt eksempel er dersom en kunde gjennom hele kundeforholdet har brukt foretakets tjenester til pensjonssparing og hverdagsbruk, plutselig sender ut store pengesummer til personer kunden aldri har sendt penger til før.[260]

I tillegg til at transaksjonsovervåking kan utløse kundetiltak i den løpende oppfølgningen, oppstiller hvvl. § 25 (2) plikt til at «[n]ærmere undersøkelser skal alltid gjennomføres dersom det avdekkes forhold som avviker fra den rapporteringspliktiges kjennskap til kunden, kundeforholdets formål og tilsiktede art». Det er nær sammenheng mellom kundetiltak i den løpende oppfølgningen, som utløses ved «tvil», jf. hvvl. § 24, og nærmere undersøkelser, som utløses ved avvik. Det følger av sammenhengen at der kundetiltakene etter hvvl. § 24 kan konstaterer avvikende kundeadferd, skal nærmere undersøkelser etter hvvl. § 25 iverksettes.

I tillegg lister hvvl. § 25 (2) opp fem kategorier av transaksjonsmodus som alltid skal undersøkes nærmere, herunder transaksjoner som

> «a. synes å mangle et legitimt formål
> b. er usedvanlig stor eller kompleks

[259] NOU 2016: 27 punkt 5.2.4.9.

[260] For flere eksempler se RTF-2022-4 s. 69–70.

c. er uvanlig ut fra kundens kjente forretningsmessige eller personlige mønster av transaksjoner

d. foretas til eller fra person i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking og terrorfinansiering

e. på annen måte har uvanlig karakter»

I Finanstilsynets rundskriv til hvitvaskingsloven gis eksempler på transaksjoner som kan falle inn under en av de opplistede vilkårene i hvvl. § 25.[261] Det følger av rundskrivet at en transaksjon som synes å mangle et legitimt formål[262] eksempelvis kan være «et oppdrag hvor pengesummen skal gå frem og tilbake mellom ulike kontoer, at samme beløp går frem og tilbake mellom ulike institusjoner, eller at en større sum splittes i flere mindre summer som samles igjen på en ny konto». En usedvanlig stor eller kompleks transaksjon[263] kan eksempelvis «dreie seg om gjennomføringen av én eller flere transaksjoner. Det kan også dreie seg om foretakets eierstruktur eller andre store og komplekse forhold». En transaksjon kan være uvanlig ut fra kundens kjente forretningsmessige eller personlige mønster av transaksjoner[264] dersom «en kunde begynner å overføre midler av en viss størrelse, eller med en viss hyppighet til utlandet, når kunden ikke har gjort dette før». Videre presiser rundskrivet at transaksjoner som foretas til eller fra en person i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking og terrorfinansiering[265] må behandles i tråd med hvitvaskingsforskriften § 4-9 bokstav c og § 4-10. Etter hvvl. §§ 4-9 og 4-10 innebærer det å underlegge kunden forsterkede kundetiltak.

I tillegg til at hvitvaskingsloven oppstiller konkrete overvåkningsforpliktelser, oppstiller hvvl. § 8 krav til å ha «oppdaterte rutiner». Det følger av bestemmelsen at formålet med rutinene er «å sikre at virksomheten håndterer identifisert risiko og oppfyller plikter etter bestemmelser gitt i eller i medhold av loven her». Plikten til å utarbeide rutiner innebærer at foretaket må utforme rutiner for hvordan foretak skal avdekke avvikende kundeadferd i overvåkingen etter hvvl. §§ 24 og 25. Som fremhevet av Finanstilsynet i tilsynspraksis må foretaket beskrive hvordan saksbehandlerne i virksomheten skal gå frem for å avdekke avvikende adferd fra foretakets kjennskap til kunden, samt de fem opplistede transaksjonsmodusene i hvvl. § 25 (2).[266]

Det følger av det ovennevnte at foretaket etter hvvl. § 8 står relativt fritt med tanke på utforming av rutiner og systemer for å avdekke avvikende kundeadferd. Det åpner opp for både bruk av elektronisk og manuell overvåking, stikkprøver, med mer. Det følger imidlertid av hvvl. § 38

[261] RFT-2022-4 punkt 6.1.1.

[262] Hvvl. § 25 (2)(a).

[263] Hvvl. § 25 (2)(b).

[264] Hvvl. § 25 (2)(c).

[265] Hvvl. § 25 (2) (d).

[266] Tilsynsrapport 20/4183.

at «[r]apporteringspliktige som nevnt i § 4 første ledd bokstav a, b og c skal ha elektroniske overvåkingssystemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering». Rapporteringspliktige etter hvvl. § 4 første ledd litra a til c vil si banker, kredittforetak og finansieringsforetak.[267] Med andre ord er banker, kredittforetak og finansieringsforetak pliktige til å anvende elektroniske overvåkingssystemer, i tillegg til å ha rutiner for overholdelse av hvvl. §§ 24 og 25, jf. hvvl. § 8. I det følgende vil jeg se nærmere på hvilke krav som stilles til utforming av det elektroniske overvåkingssystemet.

5.4.2 Plikt til å anvende elektroniske overvåkingssystemer, jf. hvvl. § 38

Plikten til å anvende elektroniske overvåkingssystemer i hvvl. § 38 er presisert i hvitvaskingsforskriften § 7-3, som spesifiserer minstekrav til hvordan det elektroniske overvåkingssystemet skal utformes. Det følger av forskriftens § 7-3 (1) at

> «[r]eglene i det elektroniske overvåkingssystemet skal være egnet til å avdekke forhold som kan indikere at midler har tilknytning til hvitvasking- og terrorfinansiering, som identifisert i den rapporteringspliktiges risikovurdering, jf. hvitvaskingsloven § 7»

Ordlyden reiser noen tolkningsspørsmål. For det første er det et spørsmål hva som menes med «regler». For det andre er det et spørsmål hvilke krav som stilles til at reglene er «egnet».

For veiledning om hva ordlyden «regler» sikter til, er det relevant å se hen til Finanstilsynets rundskriv hvor det heter at

> «[r]eglene skal være dokumentert med referanse til risikoen de er ment å redusere. Dokumentasjonen skal være versjonsstyrt slik at det er mulig på et tidspunkt tilbake i tid å se hvilke regler en transaksjon er kontrollert mot».[268]

Uttalelsen indikerer at 'regler' gir uttrykk for scenarioer identifisert med risiko for hvitvasking eller terrorfinansiering.[269] Det kan på den bakgrunn legges til grunn at regler er typetilfeller av hvitvasking og terrorfinansiering. Transaksjonsovervåkingen vil, i tråd med rundskrivet, innebære å kontrollere transaksjonen opp mot de utarbeidede scenarioene.

For det andre er det et tolkningsspørsmål hva som ligger i at reglene er «egnet». En naturlig forståelse av «egnet» er at det stilles et kvalifiserende krav. Det er dermed ikke nok at foretaket

---

[267] Etter bestemmelsens forarbeider skal kretsen av pliktsubjekter i hvvl. § 38 forstås som en henvisning til hvem som kan operere som banker, kredittforetak og finansieringsforetak etter finansforetaksloven, jf. NOU 2016:27 punkt. 8.5.5.

[268] RFT-2022-4 punkt 10.3.2.

[269] Se også Rui, Ringen, Rørholt (2022) punkt 1.2.1.

kan påvise at det har regler i det elektroniske systemet. Sett hen til at formålet med reglene etter hvitvaskingsloven § 38 er å «avdekke forhold som kan indikere hvitvasking og terrorfinansiering» trekker det i retning av at reglene rent faktisk skal kunne avdekke forhold som kan indikere at midler har tilknytning til hvitvasking- og terrorfinansiering.

Det neste spørsmålet er hvilke krav som stilles til utformingen av reglene for at de er «egnet». For det første presiserer ordlyden i forskriften § 7-3 at foretaket i utformingen av regler skal ta utgangspunkt i «forhold … identifisert i den rapporteringspliktiges risikovurdering, jf. hvitvaskingsloven § 7». Det følger av dette at for å oppfylle det kvalifiserende kravet til å ha egnede regler, må reglene reflektere risikomomentene i den rapporteringspliktiges risikovurdering.[270] I foretakets risikovurdering forventer Finanstilsynet at foretaket som et minimum tar i betraktning gjeldende «Nasjonal risikovurdering om hvitvasking og terrorfinansiering» fra Politidirektoratet og Politiets sikkerhetstjeneste (PST). I tillegg forventes det å anvende lister utarbeidet av Nasjonal tverretatlig analyse- og etterretningssenter (NTAS), og rapporter fra EU og FATF.[271] Det innebærer at reglene må reflektere risikomomentene identifisert i overnevnte rapporter.

Som kilde til utforming av regler kan foretaket også ta i bruk andre internasjonale kilder. Det er utarbeidet flere forskningsrapporter om hvitvasking og terrorfinansiering som identifiserer hovedkategorier for scenarioer, hvor det er forhøyet risiko for hvitvasking og terrorfinansiering.[272] Scenarioene som følger av denne typen rapporter kan ansees som standardscenarioer. Sett hen til at virksomheten skal ta i betraktning den konkrete risikoen virksomheten er utsatt for, jf. hvvl. § 7, må imidlertid slike standardscenarioer tilpasses markedet virksomheten operer i. Det innebærer å ta hensyn til lokale kriminalitetstrender og interne forhold ved selve virksomheten.

I den forbindelse er det spørsmål om foretaket er forpliktet til å utforme kundespesifikke regler. Kravene i forskriften til utforming av regler i overvåkingssystemet nevner ikke eksplisitt at systemet skal ta i betraktning opplysninger om den enkelte kunde. Det følger imidlertid av hvvl. §§ 24 og 25 at rapporteringspliktige skal avdekke avvikende kundeadferd. For å etterleve disse forpliktelsene er foretaket forutsetningsvis avhengig av å prioritere de kundespesifikke opplysningene i utarbeidelsen av regler. Uten innarbeidelse av kundespesifikke opplysninger fra kundetiltakene er det vanskelig å se for seg at systemet er «egnet» til å identifisere transaksjoner som kan ha tilknytning til straffbare handlinger eller terrorfinansiering, jf. hvitvaskingsforskriften § 7-3.

---

[270] Dette er også fremhevet av Finanstilsynet i RFT-2022-4 punkt 10.3.2.

[271] RFT-2022-4 punkt 2.2.4.

[272] Se eksempelvis Chau, Nemcsik (2020).

Viktigheten av at overvåkingssystemene utarbeider scenarioer og regler som kontrollerer kundens handlinger er videre fremhevet i flere tilsynsrapporter fra Finanstilsynet.[273] Søkelyset på kundespesifikke regler kan også gjenfinnes i andre land.[274] En av årsakene til at det er viktig at foretaket utarbeider kundespesifikke regler, er at transaksjonsovervåkningen ofte vil være det som danner grunnlaget for re-klassifiseringen av kunden.[275] For at foretaket kan følge opp kunden, og påse at kunden er riktig risikoklassifisert, er det nødvendig at de kundespesifikke opplysningene innarbeides i reglene.

Det neste spørsmålet er hvilke krav som stilles til individualisering av de kundespesifikke reglene. For det første må reglene være tilstrekkelig treffsikre til å avdekke «tvil om tidligere innhentede opplysninger er korrekte eller tilstrekkelige», jf. hvvl. § 24. Sett hen til den lave terskelen for å iverksette kundetiltak i den løpende oppfølgningen, må reglene være egnet til å avdekke også mindre endringer i kundeadferd.

Eksempler på hvordan foretaket kan følge opp kundens opplysninger i det elektroniske systemet er om det lages konkrete regler eller scenarioer opp mot opplysninger som den konkrete kunden har gitt. Eksempelvis at systemet genererer varsel («flagg») ved transaksjoner over angitte terskelverdier, eller andre parameter som geografi, tid og volum som kunden har sagt vedkommende vil holde seg innenfor.

For det andre er det relevant å se hen til de fem opplistede modusene i hvvl. § 25 (2). Som nevnt følger det av ordlyden at nærmere undersøkelser «alltid» skal gjennomføres dersom en transaksjon faller inn under en av de fem kategoriene av moduser. Det innebærer at foretaket må utforme kundespesifikke scenarioer som egner seg til å avdekke de fem transaksjonsmodusene i hvvl. § 25 (2).

Det reiser et spørsmål om foretaket også «alltid» må avdekke gjennomføring av en transaksjon som faller inn under en av de fem modusene, jf. ordlyden «nærmere undersøkelser skal alltid gjennomføres dersom ... en transaksjon» gir treff på en av de opplistede transaksjonsmodusene i hvvl. § 25 (2). Som et utgangspunkt følger det av den risikobaserte tilnærmingen til hvitvaskingsloven at overvåkingen kan avpasses til den enkelte kunde. Det trekker i retning av at foretaket kan avpasse reglene til den enkelte kundes risikoklassifisering, eller alternativt de ulike standardiserte risikoprofilene som foretaket operer med.

[273] Se eksempelvis tilsynsrapportene 21/668, 20/8370, 20/762.

[274] Se eksempelvis tilsynspraksis fra Sverige, jf. SEB AB 25.06.2020.

[275] RFT-2022-4 punkt 10.3.

På bakgrunn av det overnevnte kan det legges til grunn at foretaket er pliktig til å individualisere regler i langt større grad overfor høyrisikokunder enn for lavrisikokunder. Det at nærmere undersøkelser «alltid» skal iverksettes overfor de opplistede transaksjonene i hvvl. § 25 (2) indikerer imidlertid at reglene overfor den samlede kundemassen må være treffsikre nok til å utløse alarm, uavhengig av kundens risikoklassifisering.

Det følger allikevel av det jeg har gjennomgått i delkapittelet ovenfor at opplysningene rapporteringspliktige har om den enkelte kunde vil variere etter hvordan foretaket har vurdert kunderisikoen. En konsekvens av dette er at foretaket har et langt bredere kunnskapsgrunnlag for å vurdere om en transaksjon eller transaksjonsmønster er avvikende kundeadferd overfor høyrisikokunder enn for lavrisikokunder. Praktisk sett har foretaket større mulighet for å avdekke mistenkelige transaksjoner gjennomført av høyrisikokunder.

Det siste spørsmålet er hvilke forhold som kan indikere at en regel ikke er «egnet», jf. hvitvaskingsforskriften § 7-3. For hva som kan gi indikasjon på at en regel ikke er «egnet» følger det av Finanstilsynets rundskriv at «[m]ange falske positive treff på en regel kan indikere at regelen bør justeres. Ingen eller svært få treff på en regel kan også bety at regelen bør justeres, men det avhenger i større grad av hvor smalt regelen er ment å treffe».[276] Som uttalelsen i rundskrivet illustrerer må rapporteringspliktige følge opp hvor mange treff en regel får, sett opp mot hvor spesifisert regelen er ment å være.

Finanstilsynet fremhever i den sammenheng viktigheten av at disse holdes oppdaterte.[277] Scenarioene utarbeidet i systemet må følgelig revideres i takt med endringer i foretaket, eksempelvis i forbindelse med internkontroll etter hvvl. § 35. Etter hvvl. § 8 er det øverste ledelse hos den rapporteringspliktige som har ansvar for rutinene, og det skal utpekes en person i ledelsen med særskilt ansvar for å følge opp rutinene. Internkontroll med etterlevelsen etter hvvl. § 38 av regelverket er en forutsetning for at rutinene effektivt skal kunne oppdateres av øverste ledelse.[278] Internkontrollen etter hvitvaskingsloven § 35 skal gjøre foretaket i stand til å avdekke svakheter ved egen overholdelse av hvitvaskingsloven, og identifisere hva foretaket kan gjøre bedre.

5.5 Er overvåkingsforpliktelsene egnet til å oppfylle sine formål?

5.5.1 Overvåkingsforpliktelsenes klarhet og tilgjengelighet

Den risikobaserte tilnærmingen i overvåkingsforpliktelsene i hvvl. §§ 24 og 25 innebærer forutsetningsvis at den rapporteringspliktige ikke vil fange opp *alle* mistenkelige transaksjoner.

[276] RFT-2022-4 punkt 10.3.2.

[277] RFT-2022-4 punkt 10.3.2.

[278] NOU 2016: 27 side 149 og punkt 4.5.4

Samtidig får den rapporteringspliktige fleksibilitet til å bruke størsteparten av sine ressurser der det er høyest risiko for hvitvasking og terrorfinansiering. Forutsetningen for at dette systemet fungerer, er imidlertid at risikoklassifiseringen av kundene er riktig. I det følgende vil jeg argumentere for at adgangen i hvitvaskingsforskriften § 4-3 til å etablere kundeforhold med BankID ikke sikrer at rapporteringspliktige identifiserer relevant risiko virksomheten er eksponert for.

Overordnet skal bruk av en eID-ordning som oppfyller eIDAS-forordningens krav til sikkerhetsnivå 'høyt' identifisere innehaver av eID. Når noen bruker en eID er det følgelig i utgangspunktet troverdig at vedkommende er den de utgir seg for å være. Dermed er det forutsetningsvis også troverdig at det er innehaver av eID som blir kunde med foretaket, og oppgir opplysninger til foretaket. Siden BankID er en eID på høyeste sikkerhetsnivå kan løsningen brukes til å etablere kundeforhold uten supplerende tiltak.

Hvorvidt BankID faktisk oppfyller sikkerhetsnivå 'høyt' er imidlertid noe omdiskutert.[279] BankIDs sårbarhet for å bli misbrukt kan indikere at løsningen i praksis ikke gir beskyttelse tilsvarende sikkerhetsnivå 'høyt'. Det er særlig passordet tilknyttet BankID som gjør løsningen sårbar. Rapporten til Norsk senter for informasjonssikring (Norsis) om digital sikkerhetskultur fra 2023 har avdekket at 20 prosent av den norske befolkningen har latt andre bruke sin BankID, og 30 prosent av befolkningen har brukt andres BankID. Halvparten av de som har delt sin BankID, har også fått sin BankID misbrukt.[280] Det er følgelig en reell risiko for at kriminelle misbruker BankIDen til uvedkommende, og etablerer kundeforhold på vegne av innehaver av BankID. Det innebærer en risiko for følgefeil i risikoklassifiseringen av «kunden» og i transaksjonsovervåkingen av kundeforholdet.

Risikoen ligger i at «kunden» blir overvåket på bakgrunn av feil opplysninger, og under feil forutsetning om at kundeetableringen er legitim. Det innebærer en fare for at foretaket ikke avdekker potensielle hvitvaskingstransaksjoner. Risikoen aksentueres av utfordringene med misbruk av løsning for sterk kundeautentisering, som i norsk kontekst for alle praktiske formål er BankID. Når BankID misbrukes er det følgelig en kombinasjonsrisiko hvor BankID for det første kan brukes til å etablere kundeforhold, og for det andre til å gjennomføre betalingstransaksjoner.

Det reiser spørsmål om adgangen til å etablere kundeforhold med eID på høyt sikkerhetsnivå uten supplerende tiltak på tilstrekkelig måte sikrer at foretaket avdekker illegitime kundeetab-

[279] Feratovic, Leila, «ID-svindel: Sikkerhetsekspert kritiserer bankene», E24, 2. februar 2020; Se også uttalelser i FinKN-2021-36.

[280] NorSIS (2023).

leringer. Etter Finanstilsynets retningslinjer utløses krav til supplerende tiltak kun dersom overholdelse av lovens øvrige plikter til risikovurdering tilsier det. Siden nylig rettsutvikling presiserer at bruk av eID på høyt sikkerhetsnivå kan indikere lav risiko for hvitvasking og terrorfinansiering tilknyttet kundeforholdet, vil innhenting og vurdering av øvrig informasjon om kunden og kundeforholdet være avgjørende. Også her byr bruk av BankID på utfordringer.

BankID har funksjon som universalnøkkel. Det betyr at den kan benyttes som gyldig legitimasjon og autentiseringsordning overfor de fleste private og offentlige aktører.[281] Der innehaver av BankID er et frivillig pengemuldyr kan vedkommende gi alle nødvendige opplysninger til den kriminelle, eller operere under instruksjon fra den kriminelle. Der innehaver av BankID er utsatt for en identitetskrenkelse kan den kriminelle som ledd i identitetskrenkelsen lure til seg og skaffe personopplysningene om innehaver av BankID. Den med tilgang på BankIDs personlige passord kan videre logge inn i offentlige registre, hente ut opplysninger og endre opplysninger. Det innebærer at selv der den rapporteringspliktige får samtykke fra kunden til å innhente opplysninger fra offentlige registre, kan opplysningene være manipulerte.

Der et offer for misbruk av BankID er utsatt for phishingangrep er det heller ikke uvanlig at vedkommende også blir bedt om å gi fra seg personnummer. Der misbruker er en nærstående vil svindler enkelt kunne skaffe seg tilgang til denne typen informasjon, bare ved å se på betalingskortet til svindelofferet. Det er videre et anerkjent problem at lister med personinformasjon, som personnummer, selges på internett. I tillegg er navn, personnummer, adresse og øvrig personinformasjon som rapporteringspliktige skal innhente i tråd med hvvl. § 12 første ledd, typer av personlige opplysninger det er vanlig å gi fra seg – enten det er i forbindelse med kjøp på nettet, eller overfor myndighetene. Adresse er også ofte offentlig tilgjengelig informasjon.

Den kriminelle kan misbruke en kundeetablering for flere formål. Et typetilfelle er der BankID er misbrukt av den kriminelle til å ta opp lån eller kreditt, og oppretter et kundeforhold i innehaver av BankID sitt navn for deretter å flytte på utbytte fra låneopptaket. Betalingstransaksjonen av låneutbyttet vil være utbytte fra et bedrageri, og følgelig være hvitvasking.

Når kundeforholdet er underlagt transaksjonsovervåking på bakgrunn av risikovurderingen av innehaver av BankID, i stedet for den faktiske brukeren av BankID, innebærer det etter mitt syn en *betydelig* risiko for at transaksjonen ikke blir avdekket i transaksjonsovervåkingen. Dermed blir transaksjonsovervåkingsplikten forhindret fra å oppfylle sitt formål om å avdekke mistenkelige transaksjoner for å forebygge og avdekke hvitvasking og terrorfinansiering.

[281] Prop.92 LS (2019-2020) s. 184.

De iboende svakhetene til BankID taler etter mitt syn for at det er hvitvaskingsrisiko tilknyttet kundeetablering med BankID. Det kan tas til inntekt for at BankID ikke oppfyller forutsetningene til FATF for at bruk av eID til å bekrefte kundens identitet innebærer lav risiko for hvitvasking, herunder at eID-systemet er «reliable» (pålitelig) og «independent» (uavhengig), og for det andre at det er på plass «appropriate risk mitigation measures» (hensiktsmessige sikkerhetsmekanismer).[282] Det kan indikere at adgangen i Norge med kundeetablering ved bruk av BankID uten supplerende tiltak er i strid med det femte hvitvaskingsdirektivet, gjennomført i hvitvaskingsforskriften.

Ved tradisjonell etablering av kundeforhold med personlig fremmøte vil kundebehandleren kunne vurdere kundens generelle opptreden. Eksempelvis kan kundebehandler vurdere om reaksjonene på gjennomføringen av kundetiltaket avviker fra alminnelig handlemåte, og umiddelbart ha mulighet til å gjøre nærmere undersøkelser. Den fysiske nærheten mellom kundebehandler og kunde forenkler muligheten for å be om ytterligere informasjon og dokumentasjon dersom kundebehandler anser det for å foreligge risiko for hvitvasking og terrorfinansiering. De supplerende tiltakene ville kunne kompensere for fordelene ved fysisk oppmøte som går tapt når kundeetableringen skjer uten personlig fremmøte.

Det er imidlertid klart at iverksettelse av supplerende tiltak overfor alle kundeetableringer med BankID vil være byrdefullt for foretakene. Dersom foretakene skal fortsette praksisen med å tillate kundeetablering med BankID uten supplerende tiltak, burde foretakene derfor – i tråd med FATF sin anbefaling, implementere ytterligere sikkerhetstiltak i sin «management and organisation».[283]

I den forbindelse er det relevant å se hen til de nylig publiserte retningslinjene til EBA for såkalt «remote customer onboarding solutions».[284] Retningslinjene stiller både krav til finansinstitusjoners risikovurdering, overvåking av selve 'onboarding'-en, opplysningene som innhentes og koblingen mellom opplysningene og kundens identitet i verifikasjonsprosessen, når kundeetableringen skjer uten personlig fremmøte. Retningslinjene trer i kraft i EU 2. oktober 2023. Det følger av Finanstilsynets uttalelser at det forventes at norske foretak tar retningslinjene i betraktning.[285]

Jeg vil særlig fremheve at retningslinjene krever at foretaket «at least» iverksetter «ad hoc reviews» i fire angitte tilfeller, herunder

[282] FATF (2020a) avsnitt 171.

[283] FATF (2020a) avsnitt 89.

[284] EBA/GL/2022/15.

[285] Finanstilsynet, «Retningslinjer frå EBA om kundeetablering utan personleg oppmøte trer i kraft 2. oktober 2023», nyhetsmelding 23. juni 2023.

«a. changes to the ML/TF risk exposure of the credit and financial institution;
b. deficiencies on the functioning of the solution detected in the course of monitoring, audit or supervisory activities;
c. A perceived increase in fraud attempts;
d. changes to the legal or regulatory framework».[286]

Som det følger av retningslinjene er avdekkede økninger i svindelforsøk et forhold som skal innebære at foretaket iverksetter tiltak. På bakgrunn av eksplosjonen av betalingssvindel i Norge kan retningslinjene indikere at det vil være relevant for mange betalingsforetak som opererer i Norge å gjennomføre tiltak.

Jeg vil også rette noen bemerkninger til retningslinjenes krav til verifikasjonsprosedyren av nye kunder hvor «credit and financial institutions use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process». Ved kundeetablering med BankID vil kunden i de fleste tilfeller ikke interagere med en kunderådgiver. For denne typen kundeforhold skal foretaket etter retningslinjene blant annet «ensure that any photograph(s) or video is taken at the time the customer is performing the verification process», og «perform liveness detection verifications».[287] Det følger av dette at foretaket må sikre at verifikasjonsprosedyren innebærer visuelle bevis på at det faktisk er kunden som etablerer kundeforholdet.

På bakgrunn av de nye retningslinjene fra EBA burde det kunne forventes at finansforetak som har hatt en praksis med kundeetablering med BankID uten supplerende sikkerhetstiltak revurderer risikoen tilknyttet BankID, samt implementerer sikkerhetstiltakene i retningslinjen for å verifisere nye kunder.

5.5.2 Økonomiske insentiv til etterlevelse

(i) Offentligrettslig tilsyn og kontroll

Etter hvitvaskingsloven kan rapporteringspliktige som misligholder sine plikter risikere å bli ilagt overtredelsesgebyr etter hvvl. § 49 og straff etter hvvl. § 51. Det følger av tilsynspraksisen fra Finanstilsynet at gebyrene for overtredelse kan være av betydelig størrelse.[288] Det fungerer formodentlig som et effektivt «ris bak speilet».

[286] EBA/GL/2022/15, avsnitt 18.

[287] EBA/GL/2022/15, avsnitt 41.

[288] Til illustrasjon ble DNB ilagt bot på 400 millioner for manglende etterlevelse i 2021, jf. Norum, Halvar, Marthe Knudsen, «Får gigant-bot og ramsalt kritikk av Finanstilsynet», Aftenposten, 3. mai 2021.

På finanstilsynets nettsider publiseres tilsynsrapporter fra kontroll med foretakene.[289] Jeg har gjennomgått tilsyn av banker, kredittforetak og betalingsforetak i perioden 2020–2023. Forvaltningspraksisen avdekker til dels betydelige brudd på hvitvaskingslovens overvåkingsforpliktelser. Denne tendens gjenfinnes også i resten av EU.[290] På bakgrunn av tilsynsrapportene vil jeg peke på særlig to svakheter avdekket av Finanstilsynet.

En første tendens er at de rapporteringspliktige ikke identifiserer relevant risiko virksomheten er eksponert for, men i for stor grad enten baserer risikovurderingen på egne erfaringer eller på generelle, overfladiske og globale risikoer.[291] Eksempelvis avdekket tilsynet av Sparebanken Møre at banken konkluderte med lav risiko dersom banken ikke hadde eget negativt erfaringsgrunnlag.

Det er også flere tilfeller hvor tilsynet avdekker at banken er helt på den andre delen av skalaen, og ikke gjør konkrete vurderinger av iboende risikoer tilknyttet virksomheten. Det er særlig tydelig i tilsynet av Nordea Bank Adb[292] og av Eidsberg Sparebank.[293] Tilsynet kritiserer banken i begge rapportene for at risikovurderingen ikke bygger på bankens relevante data, og informasjon og erfaringer fra egen virksomhet. Finanstilsynet har også avdekket tilfeller hvor foretaket hverken tar tilstrekkelig høyde for virksomhetens iboende risiko eller risiko- og sårbarhets vurderinger fra nasjonale myndigheter og internasjonale kilder.[294]

Der banken ikke identifiserer relevant risiko og kombinasjonsrisiko oppnår ikke risikovurderingen sin tilsiktede virkning. For å beskrive faktisk risiko må det være en vekselvirkning mellom erfaringsbasert kunnskap og risikoindikatorer fra eksterne kilder.[295] Årsaken til at denne vekselvirkningen er viktig, er at dersom faktisk risiko ikke blir identifisert vil det påvirke risikoklassifiseringen av kundemassen og gjennomføringen av lovens krav til kundetiltak. Kunder som presumtivt utgjør høyere risiko blir ikke fanget opp. Basert på gjennomgangen av tilsynspraksis er det grunn til å tro at mange finansinstitusjoner ikke har tilstrekkelig forståelse av hvilken risiko foretaket er eksponert for. Følgefeilen er at foretaket ikke utarbeider scenarioer i overvåkingssystemene som fanger opp relevant risiko ved virksomheten.

---

[289] Tilsynsrapporter hvitvasking og terrorfinansiering - Finanstilsynet.no.

[290] EBA/Op/2023/08, avsnitt 5 fl.

[291] Tilsynsrapport 21/395.

[292] Tilsynsrapport 20/4183.

[293] Tilsynsrapport 21/668, hvor ble det fattet vedtak om å ilegge banken overtredelsesgebyr etter hvitvaskingsloven på 5,3 millioner kroner.

[294] Tilsynsrapport 21/668.

[295] Tilsynsrapport 20/8370.

Finanstilsynet avdekker videre at overvåkingen hos mange av bankene ikke er knyttet opp til kundespesifikke opplysninger, slik de er forpliktet til etter hvvl. § 24 og § 25. Tendensen som går igjen er at overvåkingen heller er helt generell, og kun dekker åpenbare hvitvaskingsmoduser som kontantinnskudd og -uttak, samt betalinger til og fra høyrisikoland. Til illustrasjon fant tilsynet i stikkprøvekontrollen av banken i tilsynsrapport 21/668 flere eksempler på kunder med pågående avvikende transaksjonsmønstre, sett opp mot informasjonen som forelå om kundene. Eksempelvis var det kunder med større kontantinnskudd, langt utover det som var oppgitt i kundeerklæringsskjema, uten at det hadde utløst alarmer.[296]

Det er særlig kritikkverdig at så mange av bankene underlagt tilsyn av Finanstilsynet ikke har tekniske løsninger med funksjonalitet til å vurdere kundens adferd i lys av innhentede kundeopplysninger. Resultatet er at kunder ikke blir riktig re-klassifisert sett hen til transaksjonsmønsteret. Følgefeilen innebærer at mangler i kundeinformasjon nødvendigvis også påvirker bankens evne til å bedømme hva som kan anses som kundenes normaladferd og naturlig for kundeforholdet. Et fravær av kundespesifikke regler gjør at kunder kan fortsettes å ha avvikende adferd uten at det avdekkes og videre undersøkelser iverksettes. Som Finanstilsynet også peker på, vil det medføre at mistenkelige transaksjoner ikke blir underlagt nærmere undersøkelser eller blir rapportert til Økokrim.

En årsak til den mangelfulle innsatsen kan være at det er ressurskrevende for foretaket å etterleve hvitvaskingslovens forpliktelser. Dersom det tas i betraktning at foretaket ikke bare er pålagt overvåkingsforpliktelser etter hvitvaskingsloven blir det tydelig at det totale omfanget av overvåkingsforpliktelser er betydelig.

At ikke flere av foretakene ilegges bøter kan ha sammenheng med at overtredelsesgebyr etter hvvl. § 49 er et forvaltningsvedtak med pønalt preg. Vedtak stiller krav til forvaltningens saksbehandling.[297] Dersom det skal ilegges straff etter hvvl. § 51 vil det strafferettslige legalitetsprinsippet etter Grl. § 96 gjelde. Terskelen for å sanksjonere mangelfull etterlevelse er følgelig relativt høy, og det er hovedsakelig de grovere bruddene som sanksjoneres.

Størrelsen på gebyrene er nok allikevel et betydelig insentiv til å nedlegge dokumenterbart arbeid som bevis overfor Finanstilsynet på etterlevelse av lovens forpliktelser. Det kan tas til inntekt for at tilsynets mulighet til å sanksjonere brudd har medført et økt fokus på etterlevelse

[296] Se også tilsynsrapport 20/762.

[297] Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) §§ 43 og 46, samt Grunnloven § 113.

av loven.[298] I tillegg kan det antas at banker ikke ønsker å bli assosiert med overtredelser av hvitvaskingsloven, da det kan påvirke omdømmet og verdien til foretaket.[299]

Som kartlagt innledningsvis er utfordringen med hvitvasking og digitale bedragerier imidlertid økende. Det reiser spørsmål om Finanstilsynets kontroll egner seg til å måle om foretakenes etterlevelse av loven i realiteten bekjemper hvitvasking. Gjennomgangen av tilsynspraksisen viser at Finanstilsynet i hovedsak måler etterlevelsen av hvitvaskingsloven i innsatsen foretaket legger inn i å risikovurdere egen virksomhet og kundemassen, samt iverksettelse av kundetiltak og nærmere undersøkelser basert på alarmer i overvåkingen. Jeg har eksempelvis ikke kunnet gjenfinne vurderinger i tilsynspraksisen som viser om alarmene utløst i overvåkingen reelt sett har avdekket hvitvasking.

Det er ingen nødvendig årsakssammenheng mellom det at det rapporteringspliktige formelt sett kan bevise at den nedlegger arbeid med å etterleve lovens forpliktelser og det at foretaket faktisk bekjemper hvitvasking. I diskusjonen av kundeetablering med BankID har jeg argumentert for at foretakenes etterlevelse av hvitvaskingsforskriften § 4-3 i praksis ikke er egnet til å avverge illegitime kundeetableringer, og at dette innebærer fare for følgefeil i oppfølgningen av kunden. En av årsakene til denne risikoen er at den kriminelle uten store problemer kan gi opplysninger til foretaket på en slik måte at det ikke vekker oppmerksomhet.

Hvitvaskingslovens risikobaserte tilnærming innebærer, som nevnt i punkt 8.2, at etterlevelse av loven skal avverge *risikoen for at loven ikke oppfyller sitt formål*. Formålet med loven er å avdekke og forhindre hvitvasking og terrorfinansiering, jf. hvvl. § 1. Formålet er ikke i seg selv at alle kundene beviselig er legitimert, og at foretaket kan dokumentere innhentede opplysninger om kundeforholdenes formål og tilsiktede art.

En utfordring med at tilsynet i hovedsak går ut på å undersøke om foretakene har innhentet riktige opplysninger og legitimert hele kundemassen er at de rapporteringspliktige – i frykt for sanksjoner, bruker mest ressurser på å avverge å bli ilagt bøter. Det kan stilles spørsmål ved om denne tilnærmingen er den mest effektive til å sikre at foretakene i praksis bruker nok ressurser på å forstå risikoen de er utsatt for. Dersom risikoen for hvitvasking skal bli tatt på alvor bør de rapporteringspliktige i stedet bli målt på hvor gode deres tiltak faktisk er til å identifisere og forebygge kriminalitet.

---

[298] Eksempelvis er det i DNB rundt 500 personer som arbeider i spesialistfunksjoner med å bekjempe hvitvasking og terrorfinansiering, se DNB, Antihvitvasking, antikorrupsjon og internasjonale sanksjoner.

[299] Eksempelvis falt Swedbank-aksjen 13 prosent da det ble kjent gjennom media at banken kunne ha blitt brukt til omfattende og systematisk hvitvasking, se Torset, Nina Selbo, «Stor avsløring: Swedbank anklages for storstilt hvitvasking», *Aftenposten*, 20. februar 2019.

(ii) Privatrettslig tapsrisiko som insentiv til etterlevelse

Et tiltak for å sikre at rapporteringspliktige vurderer hvor gode deres tiltak faktisk er til å identifisere og forebygge kriminalitet, er om gjennomføringen av hvitvaskingstransaksjonen innebærer tapsrisiko. Som belyst i vurderingen av overvåkingsforpliktelsene etter forskrift om systemer for betalingstjenester har pliktene som springer ut av PSD 2 hatt en betydelig svindelreduserende effekt. Jeg har i det foregående pekt på at tapsfordelingsreglene i fil. § 4-30 har vært et viktig tiltak for å oppnå dette, siden tapsfordelingsreglene sikrer at foretakets lønnsomhet blir påvirket av at det gjennomføres ikke godkjente betalingstransaksjoner.

På hvitvaskingslovens område er det imidlertid ingen tilsvarende bestemmelser som sikrer at gjennomføring av en hvitvaskingstransaksjon har direkte økonomiske konsekvenser for den rapporteringspliktige. Loven regulerer kun forholdet mellom den rapporteringspliktige og myndighetene, og kan følgelig ikke anvendes som et selvstendig ansvarsgrunnlag for bankens kunder.

6 Forholdet mellom overvåkingsforpliktelsene

Den foregående analysen har avdekket at hovedutfordringen for måloppnåelsen til overvåkingsforpliktelsene etter forskrift om systemer for betalingstjenester er utbredelsen av svindelmetoder som ikke blir fanget opp av sterk kundeautentisering. Det er manglende insentiv i tapsfordelingsreglene til å investere i systemer som egner seg til å fange opp svindeltransaksjoner autentisert med sterk kundeautentisering. Det er et spørsmål om overvåkingen etter hvitvaskingsloven kan egne seg til å avdekke svindeltransaksjoner autentisert med sterk kundeautentisering.

Det er klart at der en svindeltransaksjon er primærlovbruddet kommer ikke pliktene etter hvitvaskingsloven direkte til anvendelse på handlingen som frembringer det kriminelle utbytte. Hvitvasking er i § 2 definert som handling beskrevet i straffeloven §§ 332 og 337, og krever at handlingen er befatning med utbytte fra kriminelle handlinger. Strl. § 337 angir flere alternativer for det objektive gjerningsinnholdet, herunder å «sende» utbyttet av en straffbar handling, jf. første ledd bokstav a. Der et bedrageri skjer i bank A vil hvitvaskingshandlingen følgelig først inntre når bank A sender utbyttet fra bedrageriet til bank B. Selv om hvitvaskingsloven, på lik linje med forskrift om systemer for betalingstjenester, skal sikre hensynet til stabilitet og tillit i det finansielle systemet, springer det kriminalitetsbekjempende formålet ut fra samfunnshensyn, og ikke et direkte kundehensyn.

Når det er sagt vil beskyttelse av den enkelte kunde mot uberettiget bruk, slik som ikke godkjente transaksjoner og autorisert betalingssvindel, også ha positive ringvirkninger for samfunnet. Vice versa, ivaretakelse av samfunnshensyn innad i en finansinstitusjon vil nødvendigvis få betydning for den enkelte kunde. Sett hen til at overvåkingen etter hvitvaskingsloven skal

avdekke avvikende kundeadferd kan overvåkingen derfor i praksis være egnet til å avdekke svindeltransaksjoner.

For det første kan det sees hen til formålet med hvitvaskingsloven som er «å avdekke hvitvasking og terrorfinansiering», jf. hvvl. § 1 (1). Selv om ordlyden spesifikt retter seg hvitvasking, følger det av forarbeidene til bestemmelsen at forpliktelsene i loven at formålsbestemmelsen ikke er ment å innsnevre eller avgrense formålet med loven.[300] Videre uttales det at «hvitvaskingsloven [har] som formål ikke bare å forebygge og avdekke etterfølgende befatning med utbytte fra straffbar handling, men også å forebygge og avdekke de primærlovbrudd som utbyttet stammer fra».[301] Endringen i lovens formålsbestemmelse var ikke er en materiell endring, men en presisering av gjeldende rett. Dette ble fulgt opp av departementet.[302] På bakgrunn av det ovennevnte er det følgelig grunnlag for å fastslå at etterlevelsen av hvitvaskingslovens forpliktelser også skal kunne forebygge og avdekke primærlovbrudd – slik som eksempelvis bedragerier.

For det andre kan også samfunnshensynet som ligger til grunn for hvitvaskingsloven fremheves. Samfunnshensynet i hvitvaskingsloven skal sikre hensynet til stabilitet og tillit til det finansielle systemet som helhet. Misbruk av BankID er som fremholdt tidligere egnet til å skade kundenes tillit til betalingssystemet. Hensynet til tillit til det finansielle systemet trekker i retning av at foretaket skal avdekke nye kriminalitetsmetoder som kan skade denne tilliten, slik som bedragerier.

For det tredje kan en svindeltransaksjon rent faktisk også være befatning med utbytte fra kriminelle handlinger, og faller inn under hvitvaskingslovens definisjon av hvitvasking.[303]. Til illustrasjon kan det tenkes situasjoner med kjeder av betalingstransaksjoner som gjennomføres ved misbruk av BankID. Eksempelvis der BankID først er misbrukt til å begå et lånebedrageri, og deretter til å flytte utbytte av lånebedrageriet. Sett hen til de nære forbindelseslinjene mellom svindelrisiko og hvitvaskingsrisiko, vil jeg derfor argumentere for at det leder til et feil resultat om foretakene i utarbeidelsen av rutiner og regler i henhold til hvitvaskingsloven kan se bort ifra svindelrisiko som følge av at den risikoen skal bli håndtert av overvåkingen av ikke godkjente betalingstransaksjoner etter forordningen. En slik tilnærming innebærer at den økte risikoen for hvitvasking som følge av digitale bedragerier ikke bli fanget opp og håndtert av foretaket. Det vil være i strid med hvitvaskingslovens formål om å «avdekke og forhindre» hvitvasking, jf. § 1, og er ikke i tråd med lovens risikobaserte tilnærming etter § 6.

---

[300] Prop.40 L (2017–2018) punkt 3.3.7.1.

[301] NOU 2016: 27 s. 22.

[302] Prop.40 L (2017–2018) punkt 3.3.7.1.

[303] Prop.40 L (2017–2018) punkt 3.3.7.1.

Den praktiske virkningen av hvitvaskingsloven forutsetter at foretaket etterlever overvåkingsforpliktelsene i loven. Som avdekket i analysen av hvitvaskingsovervåkingen er det svakheter tilknyttet måloppnåelsen av hvitvaskingsloven. Jeg har argumentert for at en medvirkende faktor til dette er manglende tapsrisiko, slik som det er for ikke godkjente betalingstransaksjoner.

I den forbindelse kan det tenkes å oppstå en synergieffekt mellom hvitvaskingslovens måloppnåelse og tapsfordelingsreglene av svindeltransaksjoner. Forutsetningen er at alarmer i overvåkingen etter hvitvaskingsloven kan få betydning utover sitt anvendelsesområde. Det leder meg over til del III av avhandlingen hvor jeg vil se nærmere på betydningen av funn i transaksjonsovervåkingen.

Del III: Betydningen av funn i transaksjonsovervåkingen

7 Innledende om funn i overvåkingen

I denne delen av avhandlingen vender fokuset til betydningen av at en transaksjon eller et transaksjonsmønster blir 'flagget', herunder hvilke krav som stilles til undersøkelse av alarmer i overvåkingssystemet. Som den videre fremstillingen vil vise setter undersøkelsesforpliktelsene skranke for hvilke transaksjoner som kan gjennomføres, samt plikter dersom transaksjonen allikevel gjennomføres. I tråd med avhandlingens problemstilling vil jeg vurdere hva undersøkelsespliktene innebærer, hvordan undersøkelsespliktene forholder seg til hverandre og om de er egnet til å oppfylle sine formål.

For overvåkingsforpliktelsene regulert i forskrift om systemer for betalingstjenester følger undersøkelsespliktene av finansavtaleloven. For overvåkingsforpliktelsene etter hvitvaskingsloven regulerer hvitvaskingsloven også foretakets undersøkelsesplikter. På samme måte som i det foregående kapittelet vil jeg behandle pliktene som springer ut av de to regelsettene separat. Det innebærer at jeg først vil se på undersøkelsespliktene i finansavtaleloven (kapittel 8), før jeg ser nærmere på hvitvaskingsloven (kapittel 9). I kapittel 10 vil jeg undersøke hvordan undersøkelsespliktene forholder seg til hverandre.

8 Undersøkelsesplikter etter finansavtaleloven

8.1 Innledende bemerkninger

Etter finansavtaleloven følger skranken for gjennomføring av betalingstransaksjoner av kravet til kundens samtykke i fil. § 4-2. Samtykkekravet innebærer at en kunde kan disponere over sine midler og kontoer som de ønsker. Dersom kunden har samtykket til et betalingsoppdrag plikter kontoførende betalingstjenesteyter til å gjennomføre transaksjonen etter fil. § 4-6.

Som beskrevet i kapittel 2 må kundens samtykke være autentisert med sterk kundeautentisering for at betalingstjenesteyter kan påbegynne gjennomføringen av betalingstransaksjonen. Det innebærer at foretaket er forpliktet til å undersøke om transaksjonen er autentisert før transaksjonen sendes til oppgjøret.[304] Som utgangspunkt er det betalingstjenesteyter som har ansvar for å påvise at betalingstransaksjonen er autentisert på riktig måte. Dette er også lagt til grunn av Høyesteretts ankeutvalg i HR-2017-639-U.[305]

Ordlyden i fil. § 4-6 (1) kan videre tas til inntekt for at foretaket må kunne godtgjøre at det faktisk er tale om et «godkjent betalingsoppdrag» for at plikten til å gjennomføre transaksjonen kommer til anvendelse. De beste grunner taler dermed for at foretaket i gjennomføringen av betalingstransaksjoner har et ansvar for å undersøke om det er kunden som har autentisert initiering av betalingstransaksjonen. En naturlig følge av dette er at dersom foretaket ikke kan godtgjøre at det er snakk om et godkjent betalingsoppdrag skal foretaket ikke gjennomføre transaksjonen. På den bakgrunn skal jeg i det følgende undersøke foretakets plikt til å undersøke kundens samtykke.

For å gjøre dette vil jeg først kartlegge formålet med undersøkelsesplikten (punkt 8.2), før jeg analyserer betydningen av alarmer i overvåkingen etter henholdsvis RTS artikkel 5, 18 og 2 for foretakets undersøkelsesplikt, samt betydningen av mangelfulle undersøkelser (punkt 8.3–8.5). Til sist vil jeg undersøke i hvilken grad undersøkelsesplikten er egnet til å oppfylle sine formål (punkt 8.6).

8.2 Todelt formål: Sikre tilliten og effektivitet i betalingsformidlingen og forhindre tap som følge av ikke godkjente betalingstransaksjoner

Som kartlagt i kapittel 2 gjennomføres betalingstransaksjoner praktisk sett i oppgjøret mellom betalingsforetakene, regulert av NICS. Spørsmålet om når foretaket har adgang til å nekte å iverksette en betalingstransaksjon på bakgrunn av iverksatte undersøkelser er derfor et spørsmål om når foretaket kan tilbakekalle en betaling fra oppgjøret.

Bortfall av retten til å tilbakekalle transaksjoner er regulert av NICS. Det følger av vedlegg 1 til avtalen om avregning og oppgjør i NICS punkt 3 at «[b]anker eller tredjepart kan ikke tilbakekalle transaksjoner innsendt til NICS etter at disse anses lagt inn i NICS».[306] Det avgjørende for stansingsadgangen er følgelig tidspunktet for å legge betalingen inn i NICS.

[304] Se kapittel 2.3 for redegjørelse av oppgjørsreglene.

[305] Følger også av Finansklagenemndas praksis, se eksempelvis BKN-2007-15.

[306] Bits (2021). Vedlegg 1 til Regler for avregning og oppgjør av transaksjoner som inngår i Norwegian Interbank Clearing System (NICS), s. 2.

Vedlegg 1 til NICS regulerer ulike tidsintervaller for når en transaksjon innsendt til NICS er lagt inn i NICS. Eksempelvis, dersom en betalingstransaksjon mellom to norske banker mottas i NICS mellom kl. 09:30 og 11:30, vil NICS sende betalingen til oppgjør kl. 11:45, og betalingen formidles til bank kl 12:00.[307] De angitte tidsintervallene angir tidspunktene for å unngå og bli registrert som avvik. Transaksjonen vil derfor normalt sendes til oppgjør før de angitte fristene.[308] Det følger av det overnevnte at det er en begrenset periode betalerens betalingstjenesteyter overfor de øvrige bankene i interbanksystemet har kontraktsrettslig adgang til å tilbakekalle transaksjonen fra NICS, og herunder avstå fra å iverksette gjennomføringen av den.

Oppgjørsreglene skal sikre tilliten til gjennomføringen av transaksjoner, og effektiviteten i betalingsformidlingen.[309] Av hensyn til effektiviteten til betalingsformidlingen er det i foretakets interesse å legge til grunn at bruken av betalingsinstrumentet er legitim når det brukes sterk kundeautentisering. På den andre siden er det heller ikke i betalingsforetakenes interesse at det gjennomføres ikke godkjente betalingstransaksjoner. For det første risikerer både foretaket og kunden tap, jf. fil. § 4-30. Mer sentralt, dersom det gjennomføres for mange ikke godkjente betalingstransaksjoner svekker det kundens og samfunnets tillit til betalingssystemet.

Et mål i det påfølgende er derfor å kartlegge hvilke undersøkelser foretaket er forpliktet til å gjøre i perioden foretaket har adgang til å tilbakekalle transaksjoner fra oppgjøret. Det reiser spørsmål om hvor langt hensynet til effektivitet i betalingsformidlingen rekker, sett opp mot hensynet til kundens tillit og sikkerheten i betalingsformidlingen.

8.3 Overvåkingen etter RTS artikkel 5

Når det gjelder overvåkingen av autentiseringsprosedyren etter RTS artikkel 5 skal betalingstjenesteyter, som redegjort for i punkt 4.3, sikre sterk kundeautentifisering gjennom å overvåke tilknytningen mellom transaksjonsbeløpet, betalingsmottaker og den genererte autentifikasjonskoden gjennom hele prosessen med å gjennomføre en betalingstransaksjon. Betydningen av funn i overvåkingen av dynamisk tilknytning er regulert i RTS artikkel 5 (1)(d). Det heter i RTS artikkel 5 (1)(d) at «enhver ændring af beløbet eller betalingsmodtageren medfører, at den genererede autentifikationskode bliver ugyldig». Det er et tolkningsspørsmål hva som er betydningen av at den genererte autentifikasjonskoden «bliver ugyldig».

Isolert sett kan ordlyden «ugyldig» både sikte til juridisk ugyldighet og teknisk ugyldighet. Sett hen til at RTS er en teknisk standard, er formodentlig den tekniske betydningen av ugyldighet avgjørende. Nærmere drøftelse av hva en teknisk ugyldig autentifikasjonskode innebærer er et

[307] Bits (2021) s. 2.

[308] Bits (2021) s. 3.

[309] NOU 2017: 13 punkt 12.2.

rent teknisk spørsmål, og faller utenfor denne avhandlingen. Jeg nøyer meg derfor til å vise til RTS artikkel 4, som krever at det er generert en autentifikasjonskode for å oppfylle sterk kundeautentisering. Forutsetningsvis må autentifikasjonskoden være teknisk ´gyldig´ for at kravet til sterk kundeautentisering i RTS artikkel 4 er oppfylt. Det indikerer at en «ugyldig» autentifikasjonskode etter RTS artikkel 5 betyr at kravet til sterk kundeautentifikasjon i RTS artikkel 4 ikke lenger er oppfylt. Siden foretaket er forpliktet til å sikre kundens samtykke til initiering av elektroniske betalingstransaksjoner gjennom sterk kundeautentisering, jf. forskrift om systemer for betalingstjenester § 5, vil manglende gjennomføring av sterk kundeautentisering innebære at transaksjonen ikke er autentisert.

Det neste spørsmålet er betydningen av «ændring af beløbet eller betalingsmodtageren», jf. RTS artikkel 5 (1)(d), for vurderingen av kundens samtykke, jf. fil. § 4-2. Det alminnelige utgangspunktet for samtykke er at avgiver har samtykket til et spesifikt innhold. Ved «ændring af beløbet eller betalingsmodtageren» har det innholdsmessige grunnlaget for betalerens samtykke til initieringen av betalingstransaksjonen blitt endret. Formålet med dynamisk tilknytning er nettopp at innholdet i transaksjonen skal samsvare med det betaleren har samtykket til. Transaksjonsbeløpet og betalingsmottaker er det mest sentrale innholdet betaleren samtykker til. Det taler for at betalerens samtykke må ansees for å ha bortfalt dersom det endelige beløpet eller den endelige betalingsmottaker er endret etter at kunden har samtykket til transaksjonen.

Det neste spørsmålet er foretakets handleplikter der den dynamiske tilknytningen er brutt. Uttalelser fra EBA kan tas til inntekt for at foretaket har to handlingsalternativer. I Q&A 2020-5133 understreker EBA at kravet til dynamisk tilknytning krever at det endelige beløpet tilsvarer det autentifiserte beløpet, og uttaler videre at

> «if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction, the payer's PSP [betalingstjenestetilbyder] shall apply SCA [sterk kundeautentisering] to the final amount of the transaction or decline the transaction».

Det fremgår av uttalelsen at der det endelige beløpet ikke tilsvarer det autentiserte beløp skal betalingstjenestetilbyder enten autentisere det endelige beløp, eller avstå fra å gjennomføre transaksjonen. Uttalelsen gjelder konkret tilfeller der det endelige beløpet er ukjent når transaksjonen autentiseres. Det kan eksempelvis være tilfelle ved kjøp av dagligvarehandel på internett der kjøper godtar at det endelige beløpet vil variere på grunnlag av de faktiske kostandene for veide varer eller erstatning for utsolgte produkter. Uttalelsen har allikevel overføringsverdi, da den gir uttrykk for betalingstjenesteyters plikter i forbindelse med avdekkede avvik fra hva kunden har autentisert.

På bakgrunn av det ovennevnte kan det legges til grunn at der foretaket er forhindret fra å be om sterk kundeautentisering på nytt, skal foretaket avstå fra å gjennomføre betalingstransaksjonen og tilbakekalle transaksjonen fra oppgjøret. For å overholde sin forpliktelse til enten å be om sterk kundeautentisering på nytt eller stanse gjennomføringen av transaksjonen må foretaket agere raskt på alarmer om avdekkede endringer i den dynamiske tilknytningen.

Et siste spørsmål er betydningen av at transaksjonen allikevel gjennomføres. Basert på det ovennevnte kan det legges til grunn at dersom transaksjonen allikevel gjennomføres, uten å kreve sterk kundeautentisering på nytt, vil foretaket ha misligholdt sin forpliktelse til å kreve sterk kundeautentisering til initiering av elektroniske betalingstransaksjoner, jf. forskrift om systemer for betalingstjenester § 5.

Betydningen av foretakets pliktbrudd for tapsfordelingen er særregulert i fil. § 4-30 (5). Bestemmelsens annet punktum bokstav a til c lister opp en rekke konkrete omstendigheter som leder til at tjenesteyteren må bære tapet, med «mindre kunden har opptrådt svikaktig». Dette betyr at foretaket må dekke hele tapet, selv om kunden for eksempel har opptrådt grovt uaktsomt eller forsettlig.[310] En av omstendighetene som skal få denne virkningen er «når betalerens betalingstjenesteyter ikke har krevd sterk kundeautentisering», jf. bokstav c. Det følger av dette at dersom den dynamiske tilknytningen er brutt og foretaket hverken krever sterk kundeautentisering på nytt eller stanser gjennomføring av transaksjonen skal foretaket bære tapet i sin helhet, med mindre kunden har opptrådt svikaktig. At det også er slik kortutstedere før gjennomføringen av PSD 2 i norsk rett har praktisk reglene ved uautoriserte betalingstransaksjoner, fremheves av Entercard i høringssvar til den nye finansavtaleloven.[311]

8.4 Overvåkingen etter RTS artikkel 18

Som nevnt i del II er rettsvirkningen av at vilkårene i artikkel 18 er oppfylt at foretaket kan gjøre unntak fra kravet til sterk kundeautentisering. Realtidsovervåkingen etter artikkel 18 er følgelig et alternativ til sterk kundeautentisering. Der analysen ikke finner at transaksjonen er lav risiko, eksempelvis på bakgrunn av avdekkede funn i transaksjonsovervåkingen, kan ikke foretaket gjøre unntak fra sterk kundeautentisering.

Det følger imidlertid av sammenhengen at kravet til sterk kundeautentisering etter artikkel 18 ansees som tilstrekkelig sikkerhet mot risikoen for at transaksjonen ikke er godkjent. Det er derfor ikke holdepunkter for at funn i transaksjonsovervåkingen etter artikkel 18 har betydning

[310] Gjennomfører PSD 2 artikkel 74 (2) og (3).

[311] Prop.92 LS (2018-2019) s. 104.

for vurderingen av kundens samtykke. Dermed kan det ikke utledes noen plikt til å stanse gjennomføring av transaksjonen dersom foretaket avdekker høy risiko for svindel i realtidsanalysen etter artikkel 18. Det er nok at foretaket krever sterk kundeautentisering.

Dersom vilkårene i artikkel 18 motsetningsvis ikke er oppfylt, og foretaket allikevel gjennomfører transaksjonen, vil foretaket ha misligholdt sin plikt til å kreve sterk kundeautentisering, jf. forskrift om systemer for betalingstjenester § 5. Som redegjort for ovenfor innebærer det at foretaket skal bære tapet, med mindre kunden har opptrådt svikaktig, jf. fil. § 4-30 (5) bokstav c.

8.5 Overvåkingen etter RTS artikkel 2

8.5.1 Alarmer i overvåkningen – betydningen for autentiseringen av kundens samtykke

Et innledende spørsmål er om alarmer etter transaksjonsovervåkingen etter artikkel 2 i det hele tatt er et forhold foretaket trenger å ta i betraktning for vurderingen av om transaksjonen er autentisert. Det følger av artikkel 2 at «transaktionsovervågningsmekanismer» skal anvendes «med henblik på at gennemføre de sikkerhedsforanstaltninger, der er omhandlet i artikel 1, litra a) og b)», jf. artikkel 2. Artikkel 1(a) og (b) gjelder sikkerhetskrav påkrevd for å sikre anvendelse av sterk kundeautentisering. En naturlig forståelse av ordlyden er at det stilles krav til at betalingstjenestetilbyder har innført transaksjonsovervåkingsmekanismer for å oppfylle kravet til sterk kundeautentisering. Det antyder at transaksjonsovervåkingen inngår i oppfyllelsen av sterk kundeautentisering.

Det heter videre i første avsnitt i fortalen til forordningen at «[a]utentifikationsproceduren bør generelt omfatte transaktionsovervågningsmekanismer, som kan afsløre forsøg på at gøre brug af en betalingstjenestebrugers tabte, stjålne eller uberettiget tilegnede personaliserede sikkerhedsoplysninger, og bør også sikre, at betalingstjenestebrugeren er den retmæssige bruger, som derfor giver sit samtykke til overførslen af midler og adgang til sine kontooplysninger ved normal brug af de personaliserede sikkerhedsoplysninger». Uttalelsen retter seg mot overvåking av normal bruk av personlige sikkerhetsopplysninger. Etter RTS artikkel 2 er det som nevnt krav om overvåking av «elementer, som er typiske for betalingstjenestebrugere i forbindelse med normal brug af personaliserede sikkerhedsoplysninger». Det indikerer at uttalelsen i fortalen retter seg mot overvåkingsforpliktelsen i artikkel 2. Uttalelsen i fortalen trekker i retning av at transaksjonsovervåkingen skal inngå i autentiseringsprosedyren av transaksjonen.

Ordlyden og fortalen lest i sammenheng kan tas til inntekt for at overholdelse av overvåkingsforpliktelsen er en forutsetning for at transaksjonen er autentisert. Tolkningen innebærer at foretakets undersøkelse av alarmer i overvåkingen er en forutsetning for at foretaket kan legge til grunn at bruken av betalingsinstrumentet er legitim.

Den alternative tolkningen er at transaksjonsovervåking er et sikkerhetstiltak subsidiært til kravet til sterk kundeautentisering. Følgelig at det er tilstrekkelig for foretaket å undersøke at sterk kundeautentisering er benyttet på riktig måte. Det vil si å undersøke at det er benyttet en løsning som oppfyller kravene til sterk kundeautentisering og at dynamisk tilknytning er til stede, og eventuelt undersøke om foretaket har adgang til å gjøre unntak fra sterk kundeautentisering, jf. vurderingen ovenfor om betydningen av alarmer etter RTS artikkel 5 og 18.

På bakgrunn av ordlyden i artikkel 2 lest i sammenheng med uttalelsene i fortalen taler allikevel de beste grunner taler for at alarmer i overvåkingen etter artikkel 2 har betydning for vurderingen av autentiseringen av kundens samtykke til gjennomføringen av transaksjonen. Det vil innebære at undersøkelse av legitimiteten til bruken av sterk kundeautentisering skal inngå i foretakets vurdering av om transaksjonen er autentisert, og følgelig godkjent av kunden, jf. fil. § 4-6.

8.5.2 Betydningen av tidspunktet for overvåkingen – forholdet til reglene om oppgjør av betalingstransaksjoner

Det neste spørsmålet er betydningen av tidspunktet for overvåkingen for foretakets undersøkelsesplikt. Som diskutert i del II er overvåkingen etter artikkel 2 en etterhåndskontroll. Det innebærer at foretaket først i etterkant av gjennomføringen av transaksjonen avdekker at kunden ikke har samtykket, og herunder at transaksjonen ikke er autentisert av kunden. Etter transaksjonen allerede er gjennomført har foretaket naturligvis heller ikke adgang til å stanse gjennomføringen av den og tilbakekalle transaksjonen fra oppgjøret.

Betydningen av oppgjørsreglene for foretakets stansingsadgang kan illustreres med praksis fra Finansklagenemnda. I Finansklagenemndas praksis er det flere eksempler på kunder som i etterkant av en phishingsvindel tar kontakt med kontotilbyder og ber om at transaksjoner oppført som «reservert» stanses.[312] Det at en betaling står oppført som «reservert» er et bransjebegrep som beskriver at betalingstjenesteyter undersøker om det er dekning på konto og at det disponible beløpet blir nedjustert. Saldo forblir imidlertid uendret. Når transaksjonen belastes kontoen, blir saldo redusert og reservasjonen slettes.[313]

I samtlige saker hvor spørsmål om å stanse gjennomføringen av et reservert beløp er behandlet av nemnda har betalingstjenesteyter fått medhold i at en transaksjon oppført som «reservert»

[312] Jeg har funnet sakene ved å søke på «phishing» og «reservert» i nemdas register, og har gjennomgått sakene fra 2019 til 2023.

[313] Sharif-Askary, Jamshid (1992).

ikke kan stanses. Et eksempel er Finkn-2020-355. Kunden forklarte at han får automatisk varsling på sin telefon av alle belastningene på sitt MasterCard. Han ringte banken umiddelbart da han fikk varsel om transaksjonen. Han anførte at kontobelastningen da skulle blitt stanset. Nemnda bemerket at «en transaksjon som er reservert på kortkontoen til fordel for et brukersted i kraft av en tilsynelatende gyldig autorisasjon, ikke kan stoppes av banken etter instruks fra kortholderen». Videre kan det sees hen til Finkn-2021-107, hvor kunden oppga at banken i forkant av kundens reklamasjon hadde avdekket at transaksjonen var svindel og sperret kortet for videre transaksjoner. Banken kommenterte ikke dette. Nemnda fremholdt at «banken [ikke] kan oppheve en reservasjon selv om den i etterhånd mistenker svindel og sperrer kortet for videre transaksjoner». Lignende standardfraser er å gjenfinne i samtlige saker hvor dette spørsmålet blir reist av kunden.[314]

Grunnet de sparsommelige begrunnelsene i nemnda er det uklart hva som er bankens begrunnelse for at det ikke er mulig å stanse gjennomføringen av transaksjonen. Sett hen til at et «reservert» beløp innebærer at kundens disponible beløp er nedjustert er det imidlertid naturlig å trekke slutningen at transaksjonen er innsendt til NICS med den virkning at banken ikke har adgang til å tilbaketrekke transaksjonen fra oppgjøret.

Praksisen fra Finansklagenemnda kan imidlertid indikere at oppgjørsreglene i NICS ikke er helt absolutte. Eksempelvis i Finkn-2021-32 hadde banken – etter kundens forklaring, gitt informasjon om at mottaker av betalingen skulle kontaktes for å stanse gjennomføringen av transaksjonen. Beløpet sto ifølge kunden reservert på kontoen i flere dager før transaksjonen ble gjennomført. Banken kommenterte ikke denne delen av kortholders forklaring. Forklaringen til kunden kan imidlertid indikere at banker seg imellom har en praksis om å avtale tilbakekall av transaksjonen, selv etter at transaksjoner er innsendt til NICS.

I forlengelse av dette kan det sees hen til foretakenes samarbeidsplikt i fil. § 4-26 (2),[315] hvor det heter at «[s]elv om betalingstjenesteyteren ikke kan holdes ansvarlig etter første ledd, skal betalingstjenesteyteren treffe rimelige tiltak for å få beløpet tilbakeført. Betalingsmottakerens betalingstjenesteyter plikter å samarbeide, herunder ved å gi betalerens betalingstjenesteyter alle relevante opplysninger».[316] Bestemmelsen gjelder foretakets ansvar for betalingsoppdrag gjennomført i samsvar med det angitte kontonummeret eller annen entydig identifikasjon, der kunden har oppgitt feil opplysninger til foretaket. Det følger av bestemmelsen at på tross av at betalingstjenesteyter ikke kan holdes ansvarlig for gjennomføringen av transaksjonen, skal både

[314] Finkn-2019-39; Finkn-2019-40; Finkn-2019-939; Finkn-2020-355; Finkn-2020-455; Finkn-2021-32; Finkn-2021-107; Finkn-2021-224; Finkn-2021-426; Finkn-2021-792; Finkn-2021-838; Finkn-2021-1110; Finkn-2021-1262.

[315] Gjennomføring av PSD 2 artikkel 88 (3).

[316] Gjennomføring av PSD 2 artikkel 83 (3).

betalerens og betalingsmottakers betalingstjenesteyter bidra til å tilbakeføre transaksjonsbeløpet til betaleren.

Betalingstjenesteyter skal etter ordlyden treffe «rimelige tiltak» for å få beløpet tilbakeført jf. fil. § 4-26 (2) første punktum. Ordlyden gir ikke anvisning på konkret hva som kan forventes av foretaket. Ut ifra sammenhengen i regelverket er det allikevel naturlig at kontoførende betalingstjenesteyter forsøker å tilbakekalle transaksjonen fra oppgjøret, og ved behov ta kontakt med betalingsmottakers betalingstjenesteyter. Der betalingsmottakers betalingstjenesteyter blir kontaktet plikter denne å «samarbeide», jf. fil. § 4-26 (2) annet punktum. Det presiseres i bestemmelsen at det eksempelvis innebærer å gi «alle relevante opplysninger».

En mer-til-det-mindre-betraktning trekker i retning av at tilsvarende samarbeidsplikt må gjelde for ikke godkjente betalingstransaksjoner. Det gir liten sammenheng i regelverket om foretakene er underlagt en samarbeidsplikt der kunden har oppgitt feil opplysninger, jf. fil. § 4-26, men ikke i tilfeller der kunden ikke har samtykket til transaksjonen. Det kan tas til inntekt for at betalerens betalingstjenesteyter og betalingsmottakers betalingstjenesteyter har samarbeidsplikt også overfor ikke godkjente betalingstransaksjoner. I tråd med samarbeidsplikten i fil. § 4-26 (2) kan det innebære at betalingsmottakers betalingstjenesteyter gir relevante opplysninger som kan bidra til å opplyse forhold rundt betalerens samtykke, og at de involverte betalingstjenesteyterne søker å inngå avtale om tilbakekall av transaksjonen fra oppgjøret.

Basert på det ovennevnte kan det allikevel legges til grunn at det avgjørende for foretakets plikt til å avstå fra å gjennomføre ikke godkjente betalingstransaksjoner er om betalingstjenesteyteren blir oppmerksom på at betalingsoppdraget ikke er godkjent før transaksjonen er innsendt til NICS. Er det følgelig tale om en rekke med ikke godkjente transaksjoner, vil foretaket ha adgang til å stanse de påfølgende svindeltransaksjonene. Uavhengig av om overvåkingen skjer før eller etter gjennomføring av transaksjonen er det relevant å se nærmere på betydningen av funn i overvåkingen etter RTS artikkel 2 for vurderingen av om det er kunden som har samtykket til – og følgelig autentisert, betalingstransaksjonen.

8.5.3 Betydningen av alarmer for vurderingen av kundens samtykke

Overvåkingen etter artikkel 2 har til formål å avdekke «uautoriserte betalingstransaksjoner». Sett hen til formålet er det følgelig rimelig å anta at en alarm i systemet er en sterk indikasjon på at betalingsoppdraget ikke er godkjent av kunden. Der betaleren er utsatt for svindel – og dette fanges opp av transaksjonsovervåkingen, kan det imidlertid fortsatt være at betaleren i henhold til finansavtaleloven har samtykket til gjennomføringen av betalingstransaksjonen etter fil. § 4-2. Dette er eksempelvis tilfellet i såkalt «direktørbedrageri» hvor betaleren lures til å overføre betalingsmidler til en svindelmottaker. En alarm i overvåkingen etter artikkel 2 vil

allikevel gjøre det synbart at det er berettiget tvil om hvorvidt kunden har godkjent gjennomføring av betalingstransaksjonen.

Hverken ordlyden, fortalen eller uttalelser fra EBA gir ytterligere holdepunkter som kan kaste lys over hvilke krav som stilles til foretakets nærmere undersøkelse av alarmer i etter RTS artikkel 2. Det er dermed vanskelig å si noe generelt om akkurat hva som er skjæringspunktet for hvor mye som skal til for at foretaket må undersøke en alarm i systemet for å fastslå kundens samtykke. Sett hen til det store antallet transaksjoner som gjennomføres daglig, og det formodentlig betydelige antallet falske positiver i overvåkingen, kan det ikke nødvendigvis kreves at alle alarmer undersøkes like inngående. Det må allikevel kreves at foretaket gjennomgår alarmene og gjør en konkret vurdering.

Generelt sett kan det antas at størrelsen på avviket fra kundens normale bruk av personlige sikkerhetsanordninger har betydning for vurderingen av om kunden har samtykket. Desto større avviket er desto større grunn er det til å mistenke at kunden ikke har samtykket. Er det eksempelvis en rekke med betalingstransaksjoner som avviker fra kundens normale handlemønster, eller transaksjonene for øvrig utløser alarm på kjente svindelscenarioer eller svartelister, må alarmene få den virkning at foretaket på et tidspunkt ikke lenger kan legge til grunn at kunden har samtykket til transaksjonene.

Det reiser spørsmål om hva som kan kreves av foretaket i situasjoner der det er risiko for at kunden ikke har samtykket til transaksjonen. Sett hen til sparsommelig holdepunkter i ordlyden, fortalen og uttalelser fra EBA om foretakets undersøkelsesplikt av alarmer etter artikkel 2 er det relevant å se hen til øvrige kilder som kan kaste lys over tolkningen.

I den forbindelse er det relevant å se hen til tilbakeføringsplikten slik den er formulert i PSD 2 artikkel 73. Det heter i artikkel 73 at betalerens betalingstjenestetilbyder «i tilfælde af en uautoriseret betalingstransaktion tilbagebetaler betaleren beløbet for den uautoriserede betalingstransaktion straks og under alle omstændigheder inden afslutningen af den følgende arbejdsdag efter at have konstateret eller være blevet underrettet om transaktionen». Det følger av ordlyden at i tillegg til å ha tilbakeføringsplikt som følge av kundens varsel, har foretaket også tilbakeføringsplikt «efter at have konstateret» at transaksjonen ikke er godkjent. Ordlyden «have konstateret» gir henvisning på tilfeller hvor foretaket har objektivt konstaterbare holdepunkter for at kunden ikke har samtykket. I lys av foretakets undersøkelsesplikt ovenfor alarmer i overvåkingen kan det trekke i retning av at foretaket har en plikt til å skaffe seg konstaterbare holdepunkter ved tvil om kunden har samtykket

Det neste spørsmålet er hvordan foretaket skal gå frem for å konstatere at kunden ikke har samtykket. I den forbindelse er det relevant å se hen til varslingsplikten til foretaket, som følger

forutsetningsvis av fil. § 3-31 bokstav b. Bestemmelsen regulerer hvilke opplysninger som skal gis om sikkerhet og ansvar ved bruk av betalingstjenester. Det heter i bokstav b at foretaket skal opplyse om «en sikker prosedyre betalingstjenesteyteren kan bruke for å varsle kunden ved mistanke om eller tilfelle av svik eller sikkerhetstrusler». Bestemmelsen gjennomfører PSD 2 artikkel 52 (5)(e) som presiserer at opplysningene skal inneholde «meddelelse om en uautoriseret eller ukorrekt initieret eller gennemført betalingstransaktion i overensstemmelse med artikel 71». Det følger av direktivets ordlyd at foretaket er forpliktet til å gi opplysninger om hvordan kunden skal varsles om en ikke godkjent betalingstransaksjon. Reguleringen av opplysningsplikten indikerer at foretaket også er forpliktet til å varsle om en ikke godkjent betalingstransaksjon, der foretaket er oppmerksom på transaksjonen.

En systemorientert tolkning tilsier at det er naturlig å se varslingsplikten til foretaket i sammenheng med foretakets undersøkelsesplikt av alarmer i overvåkingen. Varselet gir foretaket anledning til å forhøre seg om bakgrunnen for transaksjonen, og avklare mistanke tilknyttet kundens samtykke. Der foretaket på bakgrunn av alarmer i overvåkingen kontakter en kunde, og vedkommende avkrefter å ha samtykket til transaksjonen, vil foretaket nettopp ha objektive konstaterbare holdepunkter for at transaksjonen ikke er godkjent av kunden.

I henhold til PSD 2 artikkel 73 innebærer det at foretaket skal tilbakeføre beløpet fra den ikke godkjente betalingstransaksjonen til kunden. Der transaksjonen ikke enda er gjennomført, eller foretaket avdekker en rekke med påfølgende svindeltransaksjoner, kan det alternativt innebære å avstå fra å sende transaksjonen til oppgjøret eller tilbakekalle transaksjonen fra oppgjøret, jf. vurderingen av foretakets stansingsplikt ovenfor.

I finansavtaleloven er foretakets tilbakeføringsplikt gjennomført i fil. § 4-32. Tilbakeføringsplikten i fil. § 4-32 gjelder «[i] den utstrekning kunden som følge av reglene i § 4-30 bestrider å ha ansvar for en ikke godkjent betalingstransaksjon». Vilkåret for tilbakeføringsplikten er at «kunden har varslet i tide etter § 4-24 annet ledd». Det heter i fil. § 4-24 at «[b]lir kunden oppmerksom på tap, tyveri eller uberettiget bruk eller tilegnelse av et betalingsinstrument eller uberettiget kontotilgang, skal kunden uten ugrunnet opphold varsle den som er oppgitt av betalingstjenesteyteren etter § 4-23 annet ledd». Foretakets plikt til å tilbakeføre tap «efter at have konstateret» at transaksjonen ikke er godkjent, jf. PSD 2 artikkel 73, er følgelig ikke å gjenfinne i finansavtalelovens gjennomføring av PSD 2.

Det kan på den bakgrunn reises spørsmål om tilbakeføringsplikten i fil. § 4-32 er gjennomført riktig. Vilkåret i fil. § 4-32 om at foretaket kun har tilbakeføringsplikt der «kunden har varslet i tide etter 4-24» kan gi et misvisende inntrykk av at foretaket ikke har forpliktelser til å klarlegge kundens samtykke på bakgrunn av overvåkingsforpliktelsene. I alle tilfeller bør derfor

foretakets varslingsplikt og kundens varslingsplikt i fil. § 4-24 sees i sammenheng. Der foretaket på bakgrunn av overvåkingen kontakter kunden for å forhøre seg om bakgrunnen for transaksjonen, og i den forbindelse avdekker at kunden bestrider å ha samtykket til transaksjonen, burde det samtidig forstås som et varsel etter fil. § 4-24 som utløser tilbakeføringsplikt etter fil. § 4-32.

8.5.4 Betydningen av misligholdte rutiner – forholdet til tapsfordelingen etter fil. § 4-30

(i) Kort om tilgang på bevis – kjennskap til foretakets etterlevelse av rutiner for overvåking

For at misligholdte rutiner skal kunne anføres av en kunde er det en forutsetning at kunden har kjennskap til foretakets etterlevelse og at instansen som skal avgjøre tapsfordelingen får fremlagt bevis som viser rutinene. Såfremt rutinene gjelder etterlevelse av pliktene etter forskrift om systemer for betalingstjenester kommer ikke taushetsplikten i hvvl. § 28 til anvendelse.[317] Det er imidlertid et spørsmål om tvisteloven § 22-10 om forretnings- og driftshemmeligheter er til hinder for bevisfremleggelse.

Spørsmålet ble reist til lagmannsretten i sak LB-2021-53168 (Borgarting). Saken er en prosessuell avgjørelse om bevisfremleggelse i tilknytning til TOSLO-2020-110915 (Oslo tingrett). Tingrettens sak gjelder tapsfordeling etter et tilfelle av «direktør-bedrageri». Det materielle spørsmålet ble anket til lagmannsretten, og avgjort i sak LB-2022-74994. Saken er sluppet inn til Høyesterett,[318] og er berammet våren 2024. Selv om det materielle spørsmålet gjelder tapsfordeling av autorisert betalingssvindel, er det prosessuelle spørsmålet om bevisfremleggelse relevant også for bevisfremleggelse av overvåkingsrutiner tilknyttet ikke godkjente betalingstransaksjoner. Om det prosessuelle spørsmålet uttalte lagmannsretten at

> «[f]lertallet ser at banken har behov for at beviset ikke tilflytes uvedkommende, som kan misbruke det. Det må imidlertid tas i betraktning at motparten i saken ikke er konkurrent og ikke vil ha noen interesse av å spre opplysningene til uvedkommende, herunder ansatte som ikke er involvert i saken».[319]

[317] Se til sml. LF-2014-9728 (Frostating); Nærmere om betydningen av foretakets taushetsplikt etter hvvl. § 28 i kapittel 10.

[318] HR-2023-1850-U.

[319] Lagmannsretten delte seg i et flertall og mindretall om hvorvidt spesifiseringen av bevisspesifikasjonen i realiteten innebar et nytt krav. Mindretallet mente anken måtte avvises, og fremsettes for tingretten som første instans. Mindretallet var imidlertid enig med flertallet tilknyttet spørsmålet om begjæringen av bevisfremleggelse skulle tas til følge.

For å avhjelpe eventuelle skadevirkninger ble de tilstedeværende pålagt taushetsplikt, og dørene ble lukket ved behandlingen av beviser. Tilsvarende betraktninger må også gjelder i saker mellom bank og kunde hvor det fremsettes begjæringer om bevisfremleggelse av rutiner for overvåking av ikke godkjente betalingstransaksjoner.

Foretakets rutiner, som i utgangspunkt er beskyttet som driftshemmeligheter, illustrerer at kunden vil støte på vansker med å ha kjennskap til foretakets etterlevelse av overvåkingsforpliktelsene. Det forvansker muligheten til å påberope misligholdt av rutinene. I det følgende vil jeg vurdere betydningen av misligholdte rutiner under forutsetningen av at kunden har anledning til å påberope seg misligholdet.

(ii) Overvåkingsforpliktelsen og kravet til sterk kundeautentisering

Som nevnt gir ordlyden i RTS artikkel 2 og fortalen holdepunkter for at transaksjonsovervåkingen inngår i autentiseringen av transaksjonen, og skal sikre sterk kundeautentisering. Det kan argumenteres for at mislighold av overvåkingsforpliktelsen dermed også skal få den virkning at sterk kundeautentisering ikke sikret på en tilstrekkelig god måte. Det at sterk kundeautentisering ikke er sikret på tilstrekkelig måte kan indikere at foretaket ikke har holdepunkter for å legge til grunn at transaksjonen er sikret med sterk kundeautentisering. Det kan tas til inntekt for at foretaket ikke kan ansees for å ha «krevd sterk kundeautentisering», jf. fil. § 4-30 (5) bokstav c. EBA har ikke kommentert om mislighold av overvåkingsforpliktelsen skal få denne virkningen. Tolkningen må følgelig ansees som usikker.

(iii) Overvåkingsforpliktelsen og vurderingen av kundens aktsomhet

Etter fil. § 4-30 (3) er kunden ansvarlig for en egenandel på 12 000 kr når tapet ved en ikke godkjent betalingstransaksjon er skjedd ved bruk av et «elektronisk betalingsinstrument» og «tapet skyldes at kunden ved grov uaktsomhet har unnlatt å oppfylle en eller flere av sine plikter etter § 4-23 første ledd eller § 4-24 første ledd».[320] At et betalingsinstrument er «elektronisk» innebærer at det er brukt et betalingsinstrument for gjennomføring av en betalingstransaksjon hvor dataene er innsamlet elektronisk, uten manuell kontroll av betalingen.[321] BankID er et eksempel på et elektronisk betalingsinstrument. Praksis fra Finansklagenemnda viser at phishing- og vishingangrep[322] er typiske tilfeller hvor det blir spørsmål om kunden har brutt sine

[320] Gjennomfører PSD 2 artikkel 74.

[321] Ot.prp. nr. 94 (2008–2009) Om lov om endringer i finansavtaleloven mv. (gjennomføring av de privatrettslige bestemmelsene i direktiv 2007/64/EF, s. 118; Ot.prp. nr. 41 (1998–1999) Om lov om finansavtaler og finansoppdrag (finansavtaleloven), s. 43.

[322] «Vishing»-angrep har likhetstrekk med phishing-angrep, idet det er en metode hvor angriperen bruker sosial manipulering for å utføre identitetstyveri. Vishing kjennetegnes at angriperen har kontakt med offeret over telefon, jf. Yeboah-Boateng, Amanor (2014) s. 297-307.

plikter ved grov uaktsomhet, siden angrepene typisk har skjedd ved bruk av et elektronisk betalingsinstrument. Det er følgelig relevant å se nærmere på betydningen av foretakets overholdelse av sikkerhetskrav for vurderingen av kundens aktsomhet.

Om vurderingen av kundens aktsomhet følger det av fortalen til PSD 2 på avsnitt 72 at «[f]or at vurdere eventuel forsømmelse eller grov forsømmelse fra betalingstjenestebrugerens side bør der tages hensyn til alle omstændigheder». I den sammenheng kan det være relevant at foretaket i RTS artikkel 2 er underlagt plikter til «at afsløre uautoriserede eller svigagtige betalingstransaktioner». Uttalelsen i fortalen til PSD 2 kan indikere at mangelfulle rutiner for å avdekke ikke godkjente betalingstransaksjoner er et relevant moment for å vurdere kundens aktsomhet.

På den andre siden knytter tapsfordelingsregelen i fil. § 4-30 (3) og PSD 2 artikkel 74 seg utelukkende til kundens handlinger. Hverken direktivet eller lovforarbeidene til finansavtaleloven kommenterer problemstillingen nærmere. Det er dermed ikke helt klart hvilken betydning foretakets overvåkingsforpliktelser skal ha for å vurdere kundens skyld.[323]

Som konstatert av Høyesterett i den såkalte «BankID»-dommen, er forhold på bankens side et relevant moment for å vurdere kundens aktsomhet i tapsfordelingen av svindelbeløp etter alminnelig erstatningsrett.[324] I den forbindelse er det relevant å se hen til forslaget til den nye forordning, som i artikkel 56 åpner opp for at «[t]he payer may be entitled to further financial compensation from the payment service provider in accordance with the law applicable to the contract concluder between the payer and the payment service provider».[325] Forslaget ser ut til å åpne opp for å utfylle tapsfordelingsreglene med nasjonale rettsregler om tapsfordeling. Det antyder at bankens overholdelse av sikkerhetsrutiner etter det nye forslaget kan inngå i aktsomhetsvurderingen av kunden, i tråd med alminnelige erstatningsrettslige prinsipper.

8.6 Er undersøkelsesplikten egnet til å oppfylle sitt formål?

8.6.1 Undersøkelsesforpliktelsens klarhet og tilgjengelighet

Analysen av foretakets undersøkelsesplikt av alarmer i overvåkingen har avdekket at det er flere uklarheter tilknyttet betydningen av alarmer etter RTS artikkel 2. Jeg har i det foregående argumentert for at foretaket på bakgrunn av funn etter overvåkingen i artikkel 2 er forpliktet til å vurdere om det faktisk er kunden som er autentisert med sterk kundeautentisering. Særlig relevant er dette for kjeder av svindeltransaksjoner, der foretaket avdekker varsler tilknyttet den eller de første svindeltransaksjonene. Undersøkelsen av alarmene, herunder varslingen til kun-

[323] For nærmere diskusjon se Amir Habibija (2022).

[324] HR-2020-2021-A, avsnitt 104.

[325] COM(2023) 367 final, artikkel 56 (6).

den, gir foretaket adgang til å stanse påfølgende svindeltransaksjoner. Det at funnene etter overvåkingen i artikkel 2 skal få betydningen som utpenslet ovenfor fremstår som en nødvendig forutsetning for det systemet PSD 2 og RTS legger opp til. Plikten til å overvåke for å avdekke ikke godkjente betalingstransaksjoner ville vært unødvendig dersom foretaket uten å undersøke alarmer i overvåkingen kan legge til grunn at bruken av et betalingsinstrument er legitim.

På grunn av hvordan norsk lovgiver har valgt å gjennomføre tilbakeføringsplikten i PSD 2 artikkel 73 vil foretak imidlertid formodentlig heller «sitte stille i båten» og avvente kundens varsel etter fil. § 4-24, enn å varsle kunden for det formål å avklare kundens samtykke. Slik jeg ser det bør ordlyden i fil. § 4-32 synliggjøre at foretaket har tilbakeføringsplikt der foretaket kan konstatere at transaksjonen ikke er godkjent, og at det innebærer at foretaket har en forpliktelse til å avklare samtykke der det er holdepunkter i overvåkingen for at det er tvil tilknyttet kundens samtykke.

8.6.2 Økonomiske insentiv til etterlevelse

Når det gjelder foretakenes tilbakeføringsplikt fremkommer det i orienteringsbrev fra forbrukertilsynet til samtlige banker i Norge at tilsynet kritiserer næringen for manglende etterlevelse av finansavtaleloven på flere punkter.[326] I gjennomgangen av etterlevelsen av tilbakeføringsplikten avdekket tilsynet blant annet at flere aktører avviste kundens reklamasjon under henvisning til at transaksjonen rent faktisk var autentisert, eksempelvis med bruk av chip og pinkode.[327]

Den avdekkede praksisen kan indikere at disse foretakene ikke på tilstrekkelig måte overvåker autentiseringen for å avdekke ikke godkjente betalingstransaksjoner (slik de er forpliktet til etter RTS artikkel 2) med den følge at foretakene ikke blir oppmerksom på risikoen for at transaksjonen ikke er autentisert av kunden. En følgeutfordring av dette er at kunden overfor betalingstjenesteyter står i en vanskelig posisjon når vedkommende skal bevise at transaksjonen ikke er godkjent, noe som kan hindre muligheten for å få tapet beløpet tilbakeført.

En årsak til dette kan være at oppfyllelse av undersøkelsesplikten skaper langt mer merarbeid og er mer ressurskrevende enn å avvente kundens varsel etter fil. § 4-24, og kreve at kunden selv sannsynliggjør at vedkommende ikke har samtykket. Det illustrerer at det er behov for at mangelfulle undersøkelser av alarmer innebærer tapsrisiko for foretaket. Det er imidlertid ikke avklart hvorvidt mangelfulle undersøkelser kan få betydning for tapsfordelingen etter fil. § 4-30. Videre er det utfordringer knyttet til kundens kjennskap til foretakets etterlevelse. Det kan forhindre at mangelfull etterlevelse blir påberopt ved tvist.

[326] Forbrukertilsynet (2022) s. 7.
[327] Forbrukertilsynet (2022) s. 5.

Det kan allikevel bemerkes at større aktører, som eksempelvis DNB, fremhever innsatsen som nedlegges i å stanse svindeltransaksjoner. Det følger av DNB sin årlige svindelrapport at banken stanset bedrageriforsøk for 1,066 millioner norske kroner i 2022, hvorpå det samlede kjente beløpet av forsøkte bedrageritransaksjoner var 1,242 millioner norske kroner.[328] Det kan indikere at (i det minste større banker som DNB) har effektive rutiner for å stanse gjennomføringen av svindeltransaksjoner.

9 Undersøkelsesplikter etter hvitvaskingsloven

9.1 Innledende bemerkninger

I dette kapittelet skal jeg se nærmere på plikten til å undersøke alarmer i overvåkningen etter hvitvaskingsloven, og hvilke handleplikter foretaket har på bakgrunn av undersøkelsene. Som et utgangspunkt følger det av hvvl. § 26 at foretaket skal rapportere «mistanke» til Økokrim. I tråd med avhandlingen tema skal jeg se på nærmere på undersøkelse av mistanke tilknyttet gjennomføring av fjernbetalingstransaksjoer.

De forutgående pliktene til å gjennomføre kundetiltak for å identifisere kundene, overvåkingen av kundeforholdet og undersøkelsene som gjennomføres på bakgrunn av overvåkingen skal sikre effektiv rapportering til Økokrim. Plikten til å rapportere kan etter dette sies å være hvitvaskingsloven kjerneforpliktelse.

For å vurdere rapporteringsplikten nærmere skal jeg kartlegge formålet med rapporteringen (punkt 9.2), før jeg ser nærmere på terskelen til rapporteringsplikten i hvvl. § 26 (punkt 9.3). Analysen vil avdekke at rekkevidden av rapporteringsplikten avhenger av foretakets nærmere undersøkelser etter hvvl. § 25. På det grunnlag vil jeg se nærmere på tidspunktet for å iverksette nærmere undersøkelser og innholdet av de nærmere undersøkelsene (punkt 9.4). Avslutningsvis vil jeg vurdere i hvilken grad undersøkelsesplikten i hvitvaskingsloven er egnet til å oppfylle sitt formål (punkt 9.5).

9.2 Formål: Gjøre myndighetene kjent med mistanken om hvitvasking

Det overordnede formålet med hvitvaskingsloven er å avdekke og forebygge hvitvaskings og terrorfinansiering, jf. hvvl. § 1 (1). Hensikten er å beskytte det finansielle og økonomiske systemet, samt samfunnet som helhet, mot skadevirkningene av hvitvasking, jf. hvvl. § 1 (2). Sikringen av hensynet til samfunnet kommer særlig til syne i forpliktelsene pålagt henholdsvis rapporteringspliktige og nasjonale myndigheter i behandlingen av opplysninger ved mistanke om hvitvasking og terrorfinansiering.

[328] DNB/FCR (2022) s. 2.

Den rapporteringspliktige skal ved mistanke om hvitvasking og terrorfinansiering rapportere til nasjonale myndigheter, og myndighetene skal benytte opplysningene i etterforskning og straffeforfølgning.[329] Effektiv overholdelse av de underliggende pliktene skal legge til rette for at rapporteringspliktige sender så riktige som mulige rapporter til myndighetene om mistanke om hvitvasking og terrorfinansiering.

En rapport til Økokrim er ikke det samme som en anmeldelse for å igangsette etterforskning.[330] Som fremhevet i årsrapporten til Enheten for finansiell etteretning (EFE), som er avdelingen i Økokrim ansvarlig for å motta rapporter, blir rapportene blir bearbeidet, beriket og analysert, og deretter formidlet til politi, tilsyns- og kontrollmyndigheter samt utenlandske samarbeidende tjenester.[331] For å bidra inn i dette er rapporteringspliktige pålagt å lagre opplysninger, og på forespørsel gi dem til myndighetene til bruk i arbeid mot profittmotivert kriminalitet.[332]

I tillegg til å rapportere mistenkelige transaksjoner til Økokrim, skal den rapporteringspliktige «avstå fra å gjennomføre mistenkelige transaksjoner før Økokrim er underrettet», jf. hvvl. § 27 (1) første punktum. Det følger av hvvl. § 27 (1) annet punktum at «Økokrim kan i særlige tilfeller forby gjennomføring av en transaksjon». Det følger av sammenhengen i bestemmelsen at foretaket kan midlertidig stanse gjennomføringen av en transaksjon, og må avvente Økokrims underretning for allikevel gjennomføre transaksjonen. Formålet med den midlertidige stansingen er at Økokrim skal få tid til å kontakte politiet og få deres vurdering av om etterforskning skal iverksettes.[333] Stansingen gjør det mulig for politiet å sikre transaksjonsbeløpet, i form av beslag eller heftelse.

Et viktig formål med rapporteringen er at den skal skje i hemmelighet, jf. det såkalte «avsløringsforbudet» i hvvl. § 28. Det innebærer at rapporteringene skal gi myndighetene informasjon, slik at de er i stand til å *forebygge* hvitvasking og terrorfinansiering, jf. hvvl. § 1. Det at rapporteringen skal bistå påtalemyndigheten i bekjempelse av hvitvasking og terrorfinansiering er styrende for tolkningen av rapporteringspliktens innhold og rekkevidde. For at rapporteringsplikten skal oppfylle sitt formål må rapporteringen skje på en slik måte og innenfor et tidsrom som gjør det mulig for påtalemyndighetene å nyttiggjøre seg av opplysningene.

[329] Økokrim/FUI (2023) s. 10.
[330] Sml. lov 22. mai 1981 om rettergangsmåten i straffesaker (straffeprosessloven) § 224.
[331] Økokrim/FUI (2023) s. 6 og 10.
[332] NOU 2016: 27 s. 22.
[333] Økokrim/FUI (2023) s. 11.

9.3 Plikt til å rapportere forhold som gir grunnlag for «mistanke» til Økokrim etter hvvl. § 26

Etter hvvl. § 26 skal rapporteringspliktige rapportere «forhold som gir grunnlag for mistanke» om hvitvasking eller terrorfinansiering. Det første spørsmålet er i hvilken grad gjennomføring av en fjernbetalingstransaksjon er et «forhold» som utløser rapporteringsplikt, jf. hvvl. § 26.

Det følger av ordlyden i hvvl. § 26 at mistanken må knytte seg til «hvitvasking eller terrorfinansiering». En naturlig språklig forståelse av ordlyden «hvitvasking» er at den rapporteringspliktige kun har rapporteringsplikt overfor hvitvaskingstransaksjoner. Det betyr at foretaket ikke har rapporteringsplikt ved mistanke om at det er begått eller vil bli begått et primærlovbrudd – med mindre det vil lede til hvitvasking.[334] Tolkningen er i tråd med lovens forarbeider.[335] Det avgrenser rapporteringspliktens rekkevidde.

Eksempelvis der en kunde er utsatt for en identitetskrenkelse hvor kontoen blir tømt kan foretakets transaksjonsovervåking gi foretaket en mistanke om at kunden er utsatt for bedrageri. Der transaksjonen fra kundens kontoførende betalingstjenestetilbyder er primærlovbruddet, vil utbyttet fra bedrageriet først være hvitvasking når beløpet sendes til betalingsmottakers betalingstjenestetilbyder.[336] Overfor denne typen transaksjoner vil kontoførende betalingstjenesteyter som et utgangspunkt ikke ha rapporteringsplikt.[337] Der transaksjonsbeløpet til sammenligning er utbytte fra et forutgående bedrageri, som utbytte fra et lånebedrageri, er transaksjonen en hvitvaskingstransaksjon som kan utløse rapporteringsplikt.

Det ovenstående illustrerer at det kan være uklare skillelinjer mellom situasjonen der foretaket står overfor «forhold som gir grunn til mistanke om hvitvasking» etter hvvl. § 26 og forhold som gir grunn til mistanke om at kunden utsettes for et primærlovbrudd. Til veiledning for å skille situasjonene uttaler hvitvaskingsutvalget i lovforarbeidene at

> «[d]en rapporteringspliktige skal stille seg spørsmålet: Er det forhold som gir grunnlag til mistanke om at virksomheten blir forsøkt brukt, brukes eller er blitt brukt som ledd i hvitvasking? Dersom det er mistanke om at midler er utbytte av en straffbar handling, skal det rapporteres».[338]

---

[334] Når det er sagt er det heller ikke noe i veien for at rapporteringspliktige anmelder slike forhold til påtalemyndigheten, jf. straffeprosessloven § 224.

[335] NOU 2016: 27 s. 225–226.

[336] Jf. strl. § 337.

[337] Betalingsmottakers betalingstjenestetilbyder vil imidlertid ha rapporteringsplikt.

[338] NOU 2016: 27 s. 225.

Det neste spørsmålet er terskelen for foretakets rapporteringsplikt. Det følger av ordlyden at rapporteringsplikten utløses ved «mistanke», jf. hvvl. § 26. Ordlyden «mistanke» er i seg selv en uklar ordlyd. Det følger imidlertid av ordlyden at foretaket har rapporteringsplikt «etter nærmere undersøkelser». Det er følgelig nær sammenheng mellom terskelen for å gjennomføre nærmere undersøkelser og terskelen for å rapportere.

Etter hvvl. § 25 skal nærmere undersøkelser gjennomføres dersom det foreligger forhold som «kan indikere» hvitvasking eller terrorfinansiering. Det er en lavere terskel enn rapporteringsplikten i hvvl. § 26, som krever at det foreligger «mistanke» om hvitvasking eller hvitvasking. Det er nærliggende å forstå sammenhengen mellom bestemmelsene dithen at foretaket har rapporteringsplikt dersom nærmere undersøkelsene ikke har avkreftet mistanken som lå til grunn for gjennomføring av de nærmere undersøkelsene.[339]

For å fastlegge rapporteringsterskelen ytterligere er det veiledende å se hen til påtalemyndighetens rett og plikt til å igangsette straffeprosessuell etterforskning. Det følger av straffeprosessloven § 224 (1) at det er tilstrekkelig med «rimelig grunn» for å undersøke om det foreligger straffbare forhold.[340] Sett hen til at formålet med rapporteringsplikten i hvitvaskingsloven er å bistå myndighetene med straffeprosessuell etterforskning, tilsier systemet at mistanketerskelen etter hvitvaskingsloven er lavere enn for straffeprosessuell forfølgning. Det ligger i dette at foretaket ikke behøver å være sikker på at midlene er kriminelt utbytte, men at det kreves mer enn generell risiko eller vage holdepunkter.

Tolkningen underbygges av uttalelser i forarbeidene, hvor hvitvaskingsutvalget fremhever at «[d]et kreves ikke sannsynlighetsovervekt».[341] Utvalget presiserer allikevel at kreves visse objektivt konstaterbare holdepunkter».[342] At det kreves visse objektivt konstaterbare holdepunkter følger også av formålet med rapporteringsplikten. Unødig rapportering vil kunne medføre unødig ressursbruk, og lede til ineffektiv bekjempelse av hvitvasking og terrorfinansiering. En slik tilnærming ville vært i strid med hvitvaskingslovens risikobaserte tilnærming.

I forarbeidsuttalelsen peker hvitvaskingsutvalget på at det må foreligge «konstaterbare holdepunkter». Det er imidlertid klart at også ett objektivt holdepunkt kan være tilstrekkelig, eksempelvis dersom en transaksjon innebærer et avvik fra normal kundeadferd som etter nærmere undersøkelser ikke kan forklares på noen god måte.[343] Når det er sagt er det klart at mistanke i

[339] Se også RFT-2022-4 punkt 6.1.

[340] Se nærmere NOU 2016: 24 Ny straffeprosesslov s. 303–304 med videre henvisninger; Nærmere redegjørelse av terskelen for å iverksette nærmere undersøkelser etter hvvl. § 25 i neste punkt.

[341] NOU 2016: 27 punkt 6.5.3.1.

[342] NOU 2016: 27 punkt 6.5.3.1.

[343] Se også uttalelser i NOU 2016:27 punkt 6.5.3.1.

mange tilfeller er avhengig av å vurdere mer enn den enkeltstående transaksjonen, eksempelvis en vurdering av kundeforholdet som helhet. Det leder meg til neste punkt, hvor jeg vil se nærmere på hvordan foretaket skal avdekke konstaterbare holdepunkter for mistanke om hvitvasking.

9.4 Iverksettelse av nærmere undersøkelser etter hvvl. § 25

9.4.1 Tidspunktet for iverksettelse av nærmere undersøkelser – forholdet til plikten til å avstå fra å gjennomføre mistenkelige transaksjoner, jf. hvvl. § 27

Som avdekket ovenfor kan foretaket konstatere at det foreligger «mistanke» etter hvvl. § 26 dersom de nærmere undersøkelsene ikke kan avkrefte mistanken som lå til grunn for de nærmere undersøkelsene etter hvvl. § 25. Spørsmålet om rekkevidden av foretakets rapporteringsplikt avhenger følgelig av tidspunktet foretaket skal iverksette nærmere undersøkelser, og innholdet i de nærmere undersøkelsene. Jeg vil først se på tidspunktet for å iverksette nærmere undersøkelser.

Etter hvvl. § 25 utløses nærmere undersøkelser dersom det avdekkes forhold som «kan indikere» at det er midler i kundeforholdet som har tilknytning til hvitvasking eller terrorfinansiering. Ordlyden legger opp til en lav terskel. Den lave terskelen gir henvisning på at det er tilstrekkelig at rapporteringspliktige har grunn til å tro at midler kan ha tilknytning til hvitvasking eller terrorfinansiering. Med andre ord at det er nok at det er grunn til å tro at midlene er utbytte fra kriminalitet, uten at det har betydning ha slags type lovbrudd utbytte stammer fra.

Denne tolkningen er i tråd med uttalelser i forarbeidene, som uttaler at «[u]ndersøkelsesplikten vil derfor kunne utløses dersom rapporteringspliktig eksempelvis har grunn til å tro at midlene er unndratt beskatning, stammer fra narkotikakriminalitet mv.».[344] Uttalelsen kan tas til inntekt for at det på tilsvarende måte er tilstrekkelig at foretaket har grunn til å tro at midlene stammer fra et bedrageri, og eksempelvis er utbytte fra en ikke godkjent betalingstransaksjon.

Terskelen for å iverksette nærmere undersøkelser etter lovens § 25 er en endring av tidligere ordlyd, der undersøkelsesplikten inntraff ved «mistanke». Ordlydsendringen var imidlertid ikke ment å være noen realitetsendring.[345] Hensikten var å tydeliggjøre forskjellen mellom undersøkelsesplikten og rapporteringsplikten. Etter forarbeidene til tidligere lovs begrepsbruk ble det uttalt at enhver mistanke i utgangspunktet kunne oppfylle kriteriet, også «diffus» mistanke.[346] Som fremhevet i proposisjonen til den nye loven vil det innebære at transaksjonsmønstre kan

[344] Prop.40 L (2017–2018) merknad til § 25, kapittel 13; Se også NOU 2016: 27 merknad til § 20, kapittel 14.1.

[345] NOU 2016: 27 punkt 6.5.2.2.1.

[346] Ot.prp. nr. 3 (2008–2009) Om lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven), punkt 5.2.3.7.

utløse undersøkelsesplikt, uten at den enkelte transaksjon i seg selv må fremstå som mistenkelig.[347]

Det at nærmere undersøkelser skal gjennomføres der den rapporteringspliktige har grunn til å tro at midlene er utbytte fra kriminalitet, innebærer imidlertid at foretaket må ha noen holdepunkter. Det er nærliggende å forstå at listen over transaksjonsmodus i hvvl. § 25 (2) angir tilfeller som alltid vil gi holdepunkter for at det foreligger forhold som «kan indikere» hvitvasking eller terrorfinansiering, jf. at ordlyden krever at nærmere undersøkelser «alltid» skal gjennomføres overfor opplistede transaksjoner.

Der en transaksjon har truffet på ett eller flere av vilkårene i hvvl. § 25 (2) uttaler Finanstilsynet videre at transaksjonen «kan også fremstå som tilforlatelige basert på kunnskap om kunden, hvilket dermed ikke utløser undersøkelsesplikt». Det følger av dette at foretaket må vurdere om treffet på ett eller flere av vilkårene faktisk er avvikende kundeadferd. Uttalelsen ser ut til å stride mot en klar ordlyd i hvvl. § 25 (2), som krever at treff på ett av vilkårene «alltid» skal undersøkes nærmere. Rekkevidden av Finanstilsynets uttalelse fremstår følgelig begrenset.

I den forbindelse reiser det seg spørsmål om hvor raskt foretaket må behandle indikasjoner på hvitvasking eller terrorfinansiering. For rapporteringspliktige som benytter elektronisk transaksjonsovervåking i henhold til hvvl. § 38 presiserer Finanstilsynet i rundskriv at «[e]nhver alarm i et transaksjonsovervåkingssystem utløser ikke undersøkelsesplikt, men alle alarmer må behandles».[348] Det følger av dette at et enkelt treff ikke umiddelbart må undersøkes nærmere. Finanstilsynet utelukker imidlertid ikke at en enkeltstående alarm *kan* utløse undersøkelsesplikt. Forutsetningen er imidlertid «at reglene i systemet er satt opp på en måte som gjør at den fanger opp atferd som treffer på ett eller flere av vilkårene i hvitvaskingsloven § 25 andre ledd». Det belyser viktigheten av at foretaket har treffsikre systemer.

Plikten til å avstå fra å gjennomføre «mistenkelige transaksjoner» inntil Økokrim er varslet om transaksjonen etter hvvl. § 27, kan gi videre veiledning for hvor raskt nærmere undersøkelser skal igangsettes. Som fremhevet i årsrapporten til Enheten for finansiell etterretning, som er avdelingen i Økokrim som mottar rapporter fra rapporteringspliktige, er formålet med å avstå fra å gjennomføre mistenkelige transaksjoner todelt.[349] For det første vil varselet forenkle etterforskningen. Når transaksjonen er gjennomført vil det være mye vanskeligere å innhente informasjon om transaksjonen. For det andre kan det sees hen til hvitvaskingslovens § 1 om å

[347] Prop.40 L (2017-2018) s. 107.
[348] RFT-2022-4 punkt 6.1.2.
[349] Økokrim/FUI (2023) s. 11.

«forhindre» hvitvasking og terrorfinansiering. Ved å stanse transaksjonen forhindrer og avverger foretaket hvitvaskings- og terrorfinansieringstransaksjoner, og gjør det enklere å inndra utbytte fra den straffbare handlingen.

Formålet med stansingsplikten kan tas til inntekt for at den beste løsningen hadde vært å innrette overvåkingen slik at transaksjonene undersøkes for det formål å avdekke mistanke *før* transaksjonen gjennomføres. Om transaksjonen i stedet kontrolleres mot regler *etter* transaksjonen er gjennomført vil plikten til å foreta nærmere undersøkelser som følge av alarm på en enkeltstående transaksjon utløses etter at pengene allerede er kommet på avveie. Da vil også mistanken om at en transaksjon er hvitvasking først avdekkes etter transaksjonen er gjennomført, med den virkning at foretaket først rapporterer om hendelsen i etterkant av gjennomføringen.

Som fremhevet av hvitvaskingsutvalget er den praktiske hovedregelen imidlertid at mistanke først underrettes til Økokrim etter transaksjonen er gjennomført.[350] Det vil i en del tilfeller være naturlig, for eksempel der mistanken om at midler stammer fra straffbare forhold eller er terrorfinansiering oppstår etter transaksjonen er gjennomført.[351] Som avdekket av EFE tar det i gjennomsnitt 2-30 dager etter nyeste transaksjon er gjennomført før mistanken rapporteres til Økokrim.[352]

Begrunnelsen for at mistenkelige transaksjoner allikevel gjennomføres, tross hovedregelen om at de skal stanses, er i ifølge lovkommentaren at «rapporteringspliktige som håndterer et stort antall kunder og transaksjoner, svært sjelden har mulighet til å følge med på og stanse transaksjoner hvor det er mistanke om hvitvasking eller terrorfinansiering i sanntid. Elektroniske overvåkingssystemer flagger transaksjoner når de er gjennomført. I tillegg kommer at jevnlige gjennomganger og kontroller ved løpende oppfølgning stort sett alltid konsentrerer seg om hendelser som har funnet sted».[353]
Det at undersøkelsen av alarmer stort sett i praksis konsentrerer seg om hendelser som har funnet sted er også i tråd med anbefalingene fra Finanstilsynet. Det heter i rundskrivet til Finanstilsynet at nærmere undersøkelser skal igangsettes «uten grunnet opphold, som i praksis betyr innen en til to dager».[354] Det at foretaket kan vente en til to dager med å igangsette nærmere undersøkelser viser at undersøkelsene ofte er en etterhåndskontroll av allerede inntrufne hendelser.

[350] NOU 2016: 27 punkt 6.5.5.
[351] NOU 2016: 27 punkt 6.5.5.
[352] Økokrim/FUI (2023) s. 39.
[353] Rui, Ringen, Rørholt (2022) punkt 2.1.5
[354] RFT-2022-4 s. 78.

> Den praktiske etterlevelsen av undersøkelsesplikten er at foretaket risikerer å medvirke til gjennomføringen av hvitvaskingstransaksjoner, jf. det lave skyldkravet i strl. § 371. Det reiser spørsmål i hvilken grad den rapporteringspliktige fremdeles har en rapporteringsplikt. Som et utgangspunkt følger det av straffeprosessloven § 232 en rett til å forholde seg taus. Siden brudd på rapporteringsplikten er straffesanksjonert og kan gi grunnlag for overtredelsesgebyr, jf. hvvl. §§ 49 og 51, må det være klart at straffeprosessloven § 232 ikke kommer til anvendelse. Det trekker med tyngde for at den rapporteringspliktige fremdeles har rapporteringsplikt, selv der foretaket har medvirket til hvitvasking. Det er imidlertid et spørsmål om hvordan dette utgangspunktet forholder seg til EMK artikkel 6 (1). Jeg avgrenser mot videre vurdering av dette spørsmålet.

9.4.2 Innholdet i de nærmere undersøkelsene

Det neste jeg skal vurdere er innholdet i de nærmere undersøkelsene. Ordlyden i hvvl. § 25 presiserer ikke hvordan foretaket skal gjennomføre de nærmere undersøkelsene. Det følger imidlertid av Finanstilsynets rundskriv til hvitvaskingsloven at undersøkelsene normalt vil ta utgangspunkt i opplysningene foretaket har om kunden, samt andre relevante tilgjengelige offentlige opplysninger.[355]

Som retningsgivende for hvilke kundetiltak foretaket kan gjennomføre er det videre relevant å se hen til «The Risk Factor Guidelines» utarbeidet av EBA. EBA fremhever at relevante kundetiltak ved forhøyet risiko for hvitvasking blant annet vil være å innhente mer informasjon fra eksterne kilder og bruke mer ressurser på egne undersøkelser.[356] I tillegg kan det være aktuelt å innhente informasjon, for eksempel ved søk i åpne kilder eller ved bistand fra en tredjepart. Nasjonalt tverretatlig analyse- og etterretningssenter (NTAS) har eksempelvis utarbeidede lister over indikatorer på mistenkelige forhold, publisert på Økokrim sine hjemmesider.[357] EU og FATF utarbeider videre jevnlige rapporter om metoder og trender som det kan forventes at rapporteringspliktige tar i betraktning.[358]

Som vist av det ovennevnte innebærer nærmere undersøkelser ikke nødvendigvis kontakt med kunden. Det henger sammen med avsløringsforbudet i hvvl. § 28. Iverksettelse av nærmere undersøkelser kan imidlertid nødvendiggjøre kontakte kunden for å få klarhet i midlenes opprinnelse.[359] Etter hvvl. § 17 vil det bety å re-klassifisere kunden til «høy risiko for hvitvasking og terrorfinansiering», og innebærer å iverksette «ytterligere «nødvendige tiltak» for å sikre kjennskap om kunden, reelle rettighetshavere og kundeforholdets formål og tilsiktede art.

---

[355] RFT-2022-4 s. 77.

[356] EBA/GL/2021/02 punkt 14.18.

[357] Publikasjoner og indikatorlister - Økokrim (okokrim.no).

[358] FATF (2020b); Commission Delegated Regulation (EU) /... amending Delegated Regulation (EU) 2016/1675 as regards adding Democratic Republic of the Congo, Gibraltar, Mozambique, Tanzania and United Arab Emirates to the table I of the Annex to Delegated Regulation (EU) 2016/1675 and deleting Nicaragua, Pakistan and Zimbabwe from that table (C(2022)9649).

[359] RFT-2022-4 s.

I tråd med hvitvaskingslovens risikobaserte tilnærming vil rekkevidden av hva som vil være «nødvendige tiltak» etter hvvl. § 17 i en konkret sak bero på en vurdering av risikoen for hvitvasking og terrorfinansiering. Det innebærer i utgangspunktet at foretaket har betydelig skjønn med hensyn til rekkevidden av kundetiltakene som gjennomføres.[360] Som lagmannsretten imidlertid fremholder i LB-2022-36100 (Borgarting) må det oppstilles visse grenser for dette skjønnet. Finanstilsynet har eksempelvis uttalt gjentatte ganger i tilsynspraksis at oversendelse av et nytt kundeerklæringsskjema ikke er tilstrekkelig forsterket kundetiltak.[361]

9.4.3 Rettsvirkningen av at forsterkede kundetiltak som ledd i nærmere undersøkelser ikke lar seg gjennomføre

Som nevnt ovenfor kan det være nødvendig å gjennomføre forsterkede kundetiltak etter hvvl. § 17 for å gjennomføre nærmere undersøkelser etter hvvl. § 25. Det reiser et spørsmål om hva foretaket skal gjøre dersom midlenes opprinnelse ikke lar seg avklare etter kontakten med kunden.

Det er relevant å se til hvvl. § 24 (4), hvor det heter at «[d]ersom kundetiltak som ledd i løpende oppfølgning ikke kan gjennomføres, skal rapporteringspliktige avvikle kundeforholdet». På bakgrunn av avviklingsplikten har foretaket rett til oppsigelse av kundeforhold etter fil. § 4-43 (1). Det er et tolkningsspørsmål hvor langt plikten til å avvikle kundeforhold rekker, og hvordan avviklingsplikten forholder seg til retten til oppsigelse etter finansavtaleloven.[362]

Formålet med kundetiltakene er å sikre at foretaket fremover i tid kan fortsette å følge opp kundeforhold, på bakgrunn av riktig risikovurdering. Midlenes opprinnelse må følgelig avklares på en slik måte at foretaket er i stand til å overvåke kunden i fremtiden. Det at foretaket avdekker forhøyet risiko for hvitvasking skal følgelig ikke i seg selv innebære at foretaket har plikt til å avvikle kundeforhold. Forhøyet risiko kan imidlertid innebære at foretaket må gjennomføre grundigere overvåking av kunden.[363]

Det følger videre av hvitvaskingsforskriften § 4-13 at foretaket i stedet for å si opp kundeforholdet kan gjennomføre mindre inngripende tiltak, som «begrense eller sperre konkrete produkter og tjenester relatert til de kundetiltak som ikke lar seg gjennomføre». Det innebærer etter sin ordlyd at foretaket eksempelvis kan hindre tilgang på den konkrete konto tilknyttet det omstridte beløpet som har utløst gjennomføringen av kundetiltak hos foretaket. På den måten kan

---

[360] Rui (2012) s. 311.

[361] Se eksempelvis tilsynsrapport 21/395.

[362] For nærmere drøftelse av skjæringspunktet for når foretakets vurdering av kundeopplysninger utløser avvisningsplikt, se Rui (2023) s. 2–49.

[363] EBA/GL/2021/02 s. 40.

foretaket hindre at kunden får tilgang til det omstridte beløpet uten at kundens kundeforhold som sådan blir berørt. Hjemmelen i hvitvaskingsforskriften § 4-13 (sammen med § 4-14) gir indirekte foretaket mulighet til å stanse gjennomføringen av transaksjoner, uten at Økokrim behøver å beslutte forbud mot å gjennomføre transaksjonen etter hvvl. § 27.[364]

9.5 Er undersøkelsesplikten egnet til å oppfylle sitt formål?

9.5.1 Undersøkelsesforpliktelsens klarhet og tilgjengelighet

Det er stigende enighet om at rammene for hvitvaskingsbekjempelse må forbedres betydelig.[365] Jeg vil knytte noen særlige bemerkninger til mistanketerskelen for å iverksette nærmere undersøkelser og rapportere til Økokrim. Som avdekket i analysen ovenfor er «mistanke» et svært vagt begrep, og iverksettelsen av nærmere undersøkelser er i stor grad opp til foretakets eget skjønn. De nærmere grensedragningene for hva som konkret utløser undersøkelsesplikten og rapporteringsplikten er uklare. Det kan enten lede til mangelfull rapportering eller overdreven rapportering. Ved mangelfull rapportering får ikke påtalemyndigheten nødvendige opplysninger for å bekjempe profittmotivert kriminalitet. Overdreven rapportering, på den andre siden, vil kunne gjøre det vanskeligere å avdekke faktiske tilfeller av hvitvasking.

Videre har analysen avdekket at det ikke oppstilles krav til samarbeid mellom betalingstjenesteyterne for å bekjempe hvitvasking. Svak informasjonsflyt om mistanke tilknyttet kunder kan svekke foretakenes mulighet til å avdekke hvitvaskingstransaksjoner, og rapportere faktiske tilfeller av hvitvasking til etterretningstjenesten.

9.5.2 Økonomiske insentiv til etterlevelse

For vurdering av foretakenes økonomiske insentiv til å etterleve forpliktelsene i hvitvaskingsloven vil jeg ta utgangspunkt i de samme tilsynsrapportene fra Finanstilsynet som gjennomgått i del II. I flere av tilsynsrapportene peker Finanstilsynet på at det ikke blir gjennomført tilstrekkelige undersøker av transaksjoner for å avkrefte mistanke. Manglene i overvåkingen kan tyde på at flere kunder skulle vært underlagt nærmere undersøkelser, og at flere transaksjoner skulle vært rapportert til Økokrim.[366] Til illustrasjon avdekker tilsynet av både Eidsberg Sparebank i rapport 21/668 og av Santander Consumer Bank i rapport 21/6151 at kunder fikk opprettholde samme mistenkelige transaksjonsmønstre over lengre tid. Begge banker ble ilagt overtredelsesgebyr.[367]

---

[364] Økokrim/FUI (2023) s. 12.

[365] Europeiske kommisjonen (2020) Meddelelse fra kommisjonen om en handlingsplan for en samlet EU-politik for forebyggelse af hvidvaskning af penge og finansiering af terrorisme.

[366] Særlig tydelig er dette i tilsynsrapport 21/668.

[367] I vedtak om overtredelsesgebyr av 28.10.2022 ble Santander Consumer Bank ilagt 150 millioner kroner i gebyr; I vedtak om overtredelsesgebyr av 26.09.2022 ble Eidsberg Sparebank ilagt 5.3 millioner kroner i gebyr.

For å unngå sanksjoner vil foretakene ha insentiver til å sende inn rapporter om mistenkelige forhold til Økokrim. Det kan i utgangspunktet være positivt. Det er allikevel et spørsmål om frykten for sanksjoner vil få den virkning at Økokrim får innsendt ugrunnede rapporter.

Det er i den forbindelse relevant å se hen til årsrapporten til EFE fra 2022, hvor det fremgår at Økokrim i løpet av 2022 mottok nesten 20 000 rapporter.[368] Det er en økning på 20 % fra året før. På bakgrunn av rapportene stanset EFE 35 transaksjoner.[369] Brorparten av rapportene leder ikke til etterforskning. Selv om det er positivt med stigende trend i antall rapporter, er det grunn til å stille spørsmål ved kvaliteten på rapportene som innsendes.

Når en rapport er sendt til Økokrim kan ikke foretaket kritiseres av tilsynet for mangelfulle undersøkelser og rapportering. Det å sikre høy kvalitet på rapportene som innsendes er imidlertid formodentlig ressurskrevende for foretaket. En uheldig virkning av en 'fryktstyrt' etterlevelse er dersom foretakene sender rapporter basert på mangelfulle undersøkelser, og der undersøkelsene viser seg å være ressurskrevende, søker å unngå å ha kunder som er ressurskrevende å følge opp.[370]

I en årrekke har EBA nettopp kritisert næringen for å praktisere de-risiking i avvikling av kundeforhold.[371] 'De-risking' innebærer at kunder som ikke er helt ordinære, utestenges fra de tjenestene rapporteringspliktige tilbyr.[372] Dersom foretakene foretar unødige kundeavviklinger vil det medføre at foretakene ikke beholder kunder hvor det er risiko for hvitvasking. For at påtalemyndigheten skal få opplysninger om denne gruppens handlinger, er det en forutsetning at disse kundene forblir kunder hos den rapporteringspliktige.[373] Unødig kundeavvikling forhindrer følgelig hvitvaskingslovens måloppfyllelse. Ønsket om å effektivisere egen drift, uten å komme i fare for sanksjoner fra tilsynet, kan være en medvirkende årsak til utfordringen med de-risking av kunder.

10 Forholdet mellom undersøkelsespliktene

10.1 Innledende bemerkninger

I forbindelse med lovarbeidet til den nye finansavtaleloven reiste flere næringsaktører i deres høringssvar bekymring omkring bevisreglene foretaket må oppfylle i forbindelse med gjennomføring av betalingstransaksjoner. Entercard fremholder at «[a]t det blir vanskeligere å verifisere

[368] Økokrim/FUI (2023) s. 3.
[369] Økokrim/FUI (2023) s. 11.
[370] Se eksempelvis Rui (2023) s. 2–49.
[371] EBA/Op/2022/01, s. 1, 4 og 6.
[372] Prop. 40 L (2017–2018) punkt 5.7.
[373] Rui (2023) s. 2–49.

betalingstransaksjoner, kan skape problemer i forhold til hvitvaskingsreglene ved at det blir lettere for den som deltar i hvitvaskingstransaksjoner å nekte ansvar».[374] I det følgende vil jeg undersøke i hvilken grad problemstillingen Entercard reiser kan oppstå i praksis.

Som avdekket i analysen skal terskelen for å iverksette undersøker på bakgrunn av funn i overvåkingen etter hvitvaskingsloven være lav. Det kan dermed tenkes at en transaksjon som må undersøkes for å fastslå kundens autentisering etter finansavtaleloven også må undersøkes for å avklare mistanke om hvitvasking. Alternativt at foretaket først avdekker at kunden hevder ikke å ha samtykket til transaksjonen i forbindelse med gjennomføring av kundetiltak etter hvitvaskingsloven.

Det reiser et innledende spørsmål om betydningen av hvitvaskingsloven undersøkelsesplikter for tapsfordelingsreglene av svindeltransaksjoner (punkt 10.2). Jeg vil både se på tapsfordelingsreglene av ikke godkjente betalingstransaksjoner etter fil. § 4-30 og tapsfordelingen av autorisert betalingsvindel etter alminnelig erstatningsrett. I forlengelsen av diskusjonen reiser det seg spørsmål om forholdet mellom foretakets varslingsplikt til kunden og taushetsplikten i hvitvaskingsloven (punkt 10.3). Videre vil jeg undersøke rekkevidden av foretakets tilbakeføringsplikt ovenfor kunden etter fil. § 4-32 i tilfeller hvor foretaket er forpliktet til å underlegge kunden kundetiltak etter hvitvaskingsloven (punkt 10.4).

10.2 Betydningen av undersøkelsesforpliktelsene i hvitvaskingsloven for tapsfordelingen av svindeltransaksjoner

10.2.1 Tapsfordelingen av ikke godkjente betalingstransaksjoner, jf. fil. § 4-30

Det første spørsmål er betydningen av hvitvaskingslovens undersøkelsesplikter for tapsfordelingen av ikke godkjente betalingstransaksjoner, jf. fil. § 4-30. Det er for det første et spørsmål om brudd på andre plikter enn dem som følger av finansavtaleloven § 4-30 (5) kan få betydning for tapsvurderingen.

Som nevnt er PSD 2 et fullharmonisert direktiv. Det betyr at medlemsstatene ikke kan beholde eller innføre regler som fraviker reglene i direktivet. Betydningen av dette er stadfestet i sak C-351/21, hvor EU-domstolen uttaler at «en parallel ansvarsordning for den samme ansvarspådragende begivenhed som en konkurrerende ansvarsordning, der gør det muligt for brugeren af betalingstjenester at gøre dette ansvar gældende på grundlag af andre udløsende begivenheder, er uforenelig med det pågældende direktiv», jf. avsnitt 37. Det følger av dette at et alternativt ansvarsregime fastsatt i nasjonal rett med hensyn til samme utløsende hendelse ikke er forenlig med direktivet. Det trekker i retning av at direktivet setter hinder for at nasjonale regler om

[374] Prop.92 LS (2018-2019) s. 104.

ansvar for pliktbrudd på betalingsforetakets side, ut over dem som følger av finansavtaleloven § 4-30 (5), kan få betydning for tapsvurderingen.

EU-domstolen uttaler videre i samme sak på avsnitt 38 at en forutsetning for å tillate at direktivets ansvarsregime eksisterer side om side med en som følger av nasjonal rett er at «denne sidstnævnte ordning ikke berører den således harmoniserede ordning og ikke er til fare for dette direktivs formål og effektive virkning». Adgangen til å ha parallelle nasjonale ansvarsregimer er følgelig svært snever. Det er etter dette tvilsomt om pliktbrudd ut over alternativene i fil. § 4-30 (5) kan oppstilles som selvstendig ansvarsgrunnlag for foretakets ansvar for tap. Som nevnt ovenfor kan det allikevel tenkes at brudd på offentligrettslige plikter kan få betydning i vurderingen av om kunden har brutt sine plikter ved grov uaktsomhet eller forsett etter fil. § 4-30 (3) og (4).[375]

10.2.2 Tapsfordelingen av autorisert betalingsvindel

Det neste spørsmålet er betydningen av hvitvaskingslovens undersøkelsesplikter for tapsfordelingen av autorisert betalingssvindel. Siden tapsfordelingen av autorisert betalingsvindel faller utenfor reguleringen i fil. § 4-30 må tapsfordelingen løses etter alminnelig erstatningsrettslige regler. I kontraktsforhold er den alminnelige erstatningsregelen culpa, som er kommet til uttrykk i skadeerstatningsloven § 2-1 om arbeidsgiveransvar. Culpa-regelen gir kunden adgang til å kreve tapet etter den autoriserte betalingstransaksjonen dekket av foretaket.

For at foretaket kan holdes ansvarlig for kundens tap på erstatningsrettslig grunnlag må det foreligge et ansvarsgrunnlag, det må ha oppstått et økonomisk tap, og det må være årsakssammenheng mellom ansvarsgrunnlaget og det økonomiske tapet. I det følgende vil jeg kort bemerke betydningen av foretakets brudd på hvitvaskingsloven for vurderingen av ansvarsgrunnlaget.

Brudd på hvitvaskingsloven er, som nevnt tidligere, ikke et selvstendig ansvarsgrunnlag. At brudd på hvitvaskingslovens forpliktelser kan være et erstatningsbetingende uaktsomt brudd på den ulovfestede profesjonsnormen følger imidlertid både i underrettspraksis[376] og av Finansklagenemnda.[377] Spørsmålet om betydningen av foretakets brudd på overvåkings- og undersøkelsesrutiner etter hvitvaskingsloven for tapsfordelingen av autorisert betalingsvindel er videre særskilt reist i den såkalte «Direktørbedrageri»-dommen.[378] Lagmannsretten delte seg i et flertall og mindretall.

---

[375] For mer om betydningen av subjektive forhold, se Amir Habibija (2022).

[376] Se eksempelvis LB-2016-20015 (Borgarting) og LE-2022-150063 (Eidsivating).

[377] Se eksempelvis FinKN-2023-592.

[378] LB-2022-74994 (Borgarting).

Med utgangspunkt i foretakets undersøkelsesplikt i hvitvaskingsloven § 25, som forutsetter at banken kjenner til kundens alminnelige transaksjonsmønster, og stansingsplikten i hvvl. § 27, uttalte flertallet at «[a]vvik fra disse kravene vil etter flertallets syn inngå som momenter i vurderingen av hva som kreves for å ha igangsatt en aktsom håndtering av svindelrisikoen». Flertallet fant følgelig grunn til å tillegge forpliktelsene i hvitvaskingsloven betydning for om foretak kan ansees å ha opptrådt uaktsom i henhold til profesjonsnormen, selv om bestemmelsene ikke kommer direkte til anvendelse.

Avgjørende for flertallet er at der overvåkingen avdekker avvikende adferd kan foretaket etter hvitvaskingsloven ikke konstatere annet enn at transaksjonen er mistenkelig. Flertallet uttalte at «[o]m det dreide seg om primærlovbrudd, selvvasking eller hvitvasking kunne de ikke vite, og det hadde de heller ikke plikt til å konkludere om. Flertallet kom til at «[t]ransaksjonene skulle ha vært vurdert opp mot de relevante røde flagg, noe banken ikke har bestridt, og de skulle etter flertallets syn ikke vært gjennomført før nærmere undersøkelse». Samlet sett kom flertallet at de manglende kontrollene var et ansvarsutløsende brudd.

Mindretallet avskjærer heller ikke at overholdelse av hvitvaskingslovens forpliktelser kan få betydning i en helhetsvurdering for om foretaket har opptrådt uaktsomt i henhold til profesjonsnormen. For at mislighold av hvitvaskingsloven alene skal gi grunnlag for erstatning må det etter mindretallets syn «i tilfelle være tale om et meget grovt brudd». Følgelig at mindre avvik ikke kan påberopes av en kunde. Både flertallet og mindretallet er følgelig enige i at etterlevelse av hvitvaskingsloven kan få betydning for vurdering av uaktsomhet etter profesjonsnormen. Lagmannsretten delte seg allikevel i synet på hvor stor betydning mangelfull etterlevelse skal få i vurderingen av foretakets uaktsomhet.

Saken har stor prinsipiell betydning for bankenes ansvar for å undersøke og overprøve kundens betalingsbeslutninger. Dersom brudd på rutiner for etterlevelse av hvitvaskingsloven får betydning for tapsfordelingen av autorisert betalingssvindel vil det kunne fungere som et effektivt økonomisk insentiv til å investere i overvåkingssystemer som egner seg til å avdekke sosial manipulasjon. I tillegg vil mangelfull etterlevelse av hvitvaskingslovens overvåkingsforpliktelser kunne påvirke foretakets bunnlinje, og fungere som insentiv til etterlevelse.

Saken har som nevnt sluppet inn for Høyesterett. Det gjenstår derfor å se hvordan Høyesterett vil vurdere rekkevidden av betalingstjenesteyteres profesjonsnorm til å avdekke og undersøke svindeltransaksjoner.

10.3 Plikten til å gjennomføre nærmere undersøkelser – forholdet til avsløringsforbudet, jf. hvvl. § 28

På bakgrunn av det overnevnte reiser det seg spørsmål om i hvilken grad avsløringsforbudet i hvvl. § 28 setter skranker for foretakets plikt til å varsle betaler om en ikke godkjent betalingstransaksjon etter finansavtaleloven og/eller gjennomføre nærmere undersøkelser etter hvitvaskingsloven.

Spørsmålet kom på spissen i sak for lagmannsretten i LB-2016-20015. Saken gjelder et erstatningskrav fra privatperson mot bank. Privatpersonen (B) hadde overlatt kodebrikken sin til kontoen i Fokus Bank til A, som hadde benyttet kodebrikken til å gjennomføre betalingstransaksjoner til Cs konto i Nordea. Fra B underslo A 9 823 381 kroner ved 65 overføringer, både i form av elektroniske betalingstransaksjoner, kontantuttak og betaling av faktura. Internt i Nordea ble det utløst varsler som ble rapportert til Økokrim, uten at C eller B sin bank ble varslet.

Spørsmålet som ble avgjort i saken var om Nordeas mangelfulle varsling til Bs bank om mistanken om at gjennomførte transaksjoner var utbytte fra bedrageri var erstatningsbetingende uaktsomt av banken. Banken anførte at hvitvaskingsloven ikke kom til anvendelse ovenfor skadelidte tredjepart, og at banken var avskåret fra å informere B eller B sin bank om alarmene i overvåkingssystemene. B på sin side anførte at Nordea hadde brutt sine plikter til å undersøke alarmene. B fremholdt at dersom alarmene hadde blitt fulgt opp med Fokus Bank, kunne denne banken på bakgrunn av undersøkelsene orientert B på en nøytral måte, og skaden ville ha blitt avverget.

Jeg vil fokusere på lagmannsrettens uttalelser om avsløringsforbudets rekkevidde. Lagmannsretten pekte på at formålet med forbudet er å hindre at arbeidet mot hvitvasking avsløres til den potensielt kriminelle kunden. Retten uttaler imidlertid at «[s]å lenge en kontakt med kunde eller tredjemann, her C, Fokus bank eller B, skjer forsiktig og nøytralt kan ikke lagmannsretten se at den vil være forbudt etter de nevnte reglene». Bankens passivitet ble på denne bakgrunn vektlagt i vurderingen av bankens erstatningsansvar. Saken ble anket til Høyesterett, men ble ikke tillatt fremmet.[379] Uttalelsen fra lagmannsretten kan følgelig ansees som uttrykk for gjeldende rett.

På bakgrunn av lagmannsrettens uttalelse kan det legges til grunn at banken ikke er avskåret fra å kontakte øvrige banker eller egne kunder på bakgrunn av mistanke om at midler i et kundeforhold er kriminelt utbytte. På tross av at hvitvaskingsloven ikke oppstiller konkrete varslingsplikter, fremgår det allikevel av lagmannsrettens begrunnelse at passivitet fra bankens side kan

[379] HR-2017-1037-U.

få betydning i vurderingen av foretakets erstatningsansvar ovenfor svindelofferet. I lys av diskusjonen ovenfor om foretakets økonomiske insentiver til etterlevelse av hvitvaskingsloven, er uttalelsen av interesse. Uttalelsen illustrerer at der tapsfordelingen av en svindeltransaksjon faller utenfor finansavtaleloven § 4-30, kan foretakets passivitet få betydning for foretakets økonomiske ansvar.

Lagmannsrettens fremhevet imidlertid at banken må utvise en viss tilbakeholdenhet for ikke å avsløre eventuell etterforskning eller varsler om hvitvasking i overvåkingssystemet. Det illustrerer at det kan oppstå potensielle motstridstilfeller i overholdelsen av foretakets plikt til å varsle om en ikke godkjent betalingstransaksjon etter finansavtaleloven, og avsløringsforbudet i hvvl. § 28.

10.4 Plikten til å tilbakeføre tap fra ikke godkjente betalingstransaksjoner til betaler etter fil. § 4-32 og risikoen for å medvirke til hvitvasking

Det følger av fil. § 4-32 (1) at der kunden «bestrider å ha ansvar for en ikke godkjent betalingstransaksjon» skal betalingstjenesteyteren «straks, og senest innen utgangen av den påfølgende virkedagen» tilbakeføre beløpet. Det følger av ordlyden «straks» at foretaket skal tilbakeføre beløpet umiddelbart. Seneste frist for å tilbakeføre er allikevel «senest innen utgangen av den påfølgende virkedagen». Ordlyden indikerer at foretaket kan gis noe tid til å gjennomføre tilbakeføringen. For å fastlegge hvilke situasjoner foretaket ikke trenger å tilbakeføre «straks» er det relevant å se hen til fil. § 4-32 (2).

Det heter i annet ledd at «[f]ørste ledd gjelder ikke dersom betalingstjenesteyteren har rimelige grunner til mistanke om svik». Ordlyden «svik» peker på situasjoner der kunden forsøker å utnytte finansforetakets tjenester. Det at kunden utgir seg for å være et svindeloffer, men i realiteten har gjennomført en hvitvaskingstransaksjon, er klart svikaktig. Det kan på den bakgrunn legges til grunn at foretaket ikke vil ha tilbakeføringsplikt etter første ledd overfor kunden som deltar i hvitvaskingstransaksjoner.

Unntaket fra tilbakeføringsplikten gjelder der foretaket har «rimelige grunner til mistanke om svik». Ordlyden «rimelig grunn til mistanke» indikerer at foretaket har konkrete holdepunkter som gir grunn til å mistenke kunden for å opptre svikaktig. Det er nærliggende å forstå sammenhengen i regelverket at foretaket etter fil. § 4-32 (1) får «innen utgangen av påfølgende virkedag» til å undersøke mistanken om svik nærmere. Har foretaket ikke har avkreftet mistanken innen denne fristen, har foretaket ikke tilbakeføringsplikt etter fil. § 4-32.

Etter Finanstilsynets rundskriv skal foretaket igangsette nærmere undersøkelser etter hvitvaskingsloven i løpet av en til to virkedager etter transaksjonen utløser alarm. Det er ingen tidsfrister i hvitvaskingsloven for når foretaket skal være ferdig med de nærmere undersøkelsene.

Det kan følgelig tenkes situasjoner der foretaket ikke får avkreftet mistanken om hvitvasking etter nærmere undersøkelser «innen utgangen av påfølgende virkedag» etter kundens reklamasjon, jf. fil. § 4-32 (1).

Det reiser et spørsmål om foretakets tilbakeføringsplikt er bortfalt i sin helhet i situasjoner der foretaket ikke har avkreftet mistanken om hvitvasking «innen utgangen av påfølgende virkedag» etter kundens reklamasjon, jf. fil. § 4-32 (1). Terskelen for at foretaket ikke lenger har tilbakeføringsplikt etter fil. § 4-32 (1) er som nevnt at foretaket har «rimelige grunner til mistanke om svik», jf. fil. § 4-32 (2). Til sammenligning er terskelen etter hvitvaskingsloven § 25 for å igangsette nærmere undersøkelser av en transaksjon at det foreligger forhold som «kan indikere» hvitvasking eller terrorfinansiering. Som fastslått i redegjørelsen av undersøkelsespliktens innhold kreves det visse objektivt konstaterbare holdepunkter.[380] Terskelen for unntaket til tilbakeføringsplikten i fil. § 4-32 har følgelig store likhetstrekk med terskelen for å igangsette undersøkelser etter hvvl. § 25.

Ordlyden i fil. § 4-32 (2) må imidlertid forstås dithen at unntaket fra tilbakeføringsplikten kun gjelder *så lenge* foretaket har «rimelige grunner til mistanke om svik». Der de nærmere undersøkelsene etter hvitvaskingsloven avkrefter mistanken om hvitvasking taler de beste grunner for at det er hovedregelen i fil. § 4-32 (1) som gjelder, som bestemmer at foretaket skal tilbakeføre «straks». Det trekker i retning av foretaket har tilbakeføringsplikt umiddelbart etter foretaket har avkreftet mistanken om hvitvasking etter hvvl. § 25.

Del IV: Avsluttende bemerkninger

Analysen av overvåkingsforpliktelsene har avdekket spenninger mellom foretakenes effektivitetssøken og hensynene til å beskytte kunden og samfunnet mot kriminell utnyttelse av betalingssystemet. Når det gjelder hvitvaskingsloven er det avdekket flere forhold som kan svekke måloppnåelsen. For det første er det grunnlag for å kritisere foretakene for mangelfull etterlevelse av hvitvaskingsloven. En av årsakene er at pliktene i hvitvaskingsloven reiser mange tolkningsspørsmål som ikke er tilstrekkelig klargjort av EU eller norsk lovgiver. Gjennomgangen belyser også at det er utfordringer med tilsynsmyndighetenes mulighet til å følge opp foretakene på en måte som sikrer etterlevelse. I tillegg er det grunn til å kritisere adgangen i hvitvaskingsforskriften til å etablere kundeforhold med BankID uten supplerende tiltak. Unntaksadgangen undergraver potensielt effektiviteten til overvåkingsforpliktelsene etter både forskrift om systemer for betalingstjenester og hvitvaskingsloven, da foretaket ikke på tilstrekkelig måte sikrer legitimiteten til kontoen og opplysningene om kunden.

[380] NOU 2016: 27 punkt 6.5.3.1.

Når det gjelder sikkerhetskravene til sterk kundeautentisering har avhandlingen avdekket at EU i utformingen av sikkerhetskravene har lagt vekt på innovasjon og konkurranse om sikkerheten til betalingskontoene. Betalingstjenesteleverandørene har rett til å stole på autentiseringsprosessen til banken. Betalingstjenesteleverandørene har imidlertid frihet til å arrangere autentiseringen slik de finner mest hensiktsmessig. Banken har kun begrensede muligheter for å begrense tilgangen til kontoer og stanse gjennomføringen av transaksjoner.

Analysen av undersøkelsespliktene i finansavtaleloven som springer ut av PSD 2 kan indikere at utviklingen av markedet for betalingstjenester blir prioritert fremfor sikkerheten til betalingskontoen. Dette betyr ikke automatisk at kundene ikke er tilstrekkelig beskyttet. Til syvende og sist avhenger sikkerheten til kunden av oppfyllelsen av sikkerhetskravene til autentiseringen av betalingstransaksjoner og tredjeparters tilgang på betalingskonten. Det fordrer at foretakene har tilstrekkelige insentiver til å etterprøve initieringen av betalingstransaksjoner, og til å undersøke legitimiteten til autentiseringen av kundens samtykke.

Tapsfordelingsreglene etter finansavtaleloven og på culpa-grunnlag har en viktig funksjon som insentiv til etterlevelse av sikkerhetskravene. Avhandlingen har imidlertid avdekket at det er utfordringer og uløste spørsmål tilknyttet tapsfordelingsreglene. Jeg har skissert noen av spørsmålene som kan oppstå, som utfordringene med foretakenes taushetsplikt etter hvvl. § 28 i overholdelsen av varslingspliktene i hvitvaskingsloven og finansavtaleloven. Spørsmål om taushetsplikten til foretaket kan også få betydning for kundens mulighet til å kreve bevisfremleggelse av foretakets etterlevelse av rutiner for overvåking og undersøkelse. Det kan forhindre kundens mulighet til å påberope foretakenes brudd på pliktene i rettssystemet.

Det er videre andre grensedragningsspørsmål som avhandlingen ikke har hatt anledning til å undersøke nærmere. Et slikt spørsmål er rekkevidden av foretakets adgang til å fryse kontomidler, jf. hvitvaskingsforskriften § § 4-13, i etterlevelsen av foretakenes plikt til å samarbeide om å tilbakeføre tap etter en ikke godkjent betalingstransaksjon til svindelofferet.

For å effektivt bekjempe utfordringen med digitale bedragerier og hvitvasking er det nødvendig at disse utfordringene håndteres. Som kartlagt i avhandlingen er det stadig rettsutvikling fra EU med sikte på å avverge de fremvoksende sikkerhetsutfordringene. Det er av sentral betydning at rettsutviklingen følges opp både på regulatorisk nivå, i rettspraksis og av næringen selv.

Litteraturliste

LOV, FORSKRIFT OG FORARBEIDER:

Kongeriket Norges Grunnlov 17. mai 1814 (Grunnloven).

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

Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

Lov 18. desember 2020 nr. 146 om finansavtaler (finansavtaleloven – fil.).

Lov 20. mai 2005 nr. 29 om straff (straffeloven – strl.).

Lov 22. mai 1981 om rettergangsmåten i straffesaker (straffeprosessloven).

Lov 23. november 2018 nr. 87/2018 om endringer i finansforetaksloven mv.

Lov av 9. januar 2009 nr. 2 om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven).

Forskrift 5. juni 2023 nr. 1245 om endring i forskrift om systemer for betalingstjenester.

Forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon 21. november 2019 nr. 1578 (selvdeklarasjonsforskriften); Selvdeklarasjonsforskriften definerer sikkerhetsnivåer og tilsynsregime for elektroniske identifikasjonsordninger (eID-ordninger).

Forskrift om systemer for betalingstjenester 15. februar 2019 nr. 152.

Forskrift om tiltak mot hvitvasking og terrorfinansiering 14. september 2019 nr. 1324 (hvitvaskingsforskriften).

NOU 1996: 24 Betalingssystemer m.v. Utredning nr 3 fra Banklovkommisjonen.

NOU 2002: 4 Ny straffelov Straffelovkommisjonens delutredning VII.

NOU 2016: 27 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering andre delutredning.

NOU 2017: 13 Ny sentralbanklov. Organisering av Norges Bank og Statens pensjonsfond utland.

Ot.prp. nr. 3 (2008–2009) Om lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven).

Ot.prp. nr. 41 (1998–1999) Om lov om finansavtaler og finansoppdrag (finansavtaleloven).

Ot.prp. nr. 94 (2008–2009) Om lov om endringer i finansavtaleloven mv. (gjennomføring av de privatrettslige bestemmelsene i direktiv 2007/64/EF.

Prop.92 LS (2019–2020) Lov om finansavtaler (finansavtaleloven) og samtykke til godkjennelse av EØS-komiteens beslutninger nr. 125/2019 og 130/2019 av 8. mai 2019 om innlemmelse i EØS-avtalen av direktiv 2014/17/EU om kredittavtaler for forbrukere i forbindelse med fast eiendom til boligformål (boliglåndirektivet) og delegert kommisjonsforordning (EU) nr. 1125/2014.

RETTSAKTER FRA EU/EØS:

Vedtatte rettsakter

Europaparlaments- og rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF. (PSD 2).

Europaparlamentets- og rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF. (det fjerde hvitvaskingsdirektivet – 4AMLD).

Europaparlamentets rådsdirektiv (EU) 2018/843 af 30. maj 2018 om ændring af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme og om ændring af direktiv 2009/138/EF og 2013/36/EU. (det femte hvitvaskingsdirektivet – 5AMLD).

Europarlamentets- og rådets direktiv (EU) Nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF. (oprettelsesforordningen).

EØS-tillegget til Den europeiske unions tidende Nr. 34/61. (2023/EØS/34/17).

Commission Delegated Regulation (EU) /... amending Delegated Regulation (EU) 2016/1675 as regards adding Democratic Republic of the Congo, Gibraltar, Mozambique, Tanzania and United Arab Emirates to the table I of the Annex to Delegated Regulation (EU)

2016/1675 and deleting Nicaragua, Pakistan and Zimbabwe from that table. (C(2022)9649).

Europaparlamentets rådsdirektiv (EU) No 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF. (eIDAS).

Delegert kommisjonsforordning (EU) 2018/389 af 27. november 2017 om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation. (RTS).

Europaparlamentets- og rådets direktiv 2007/64/EC af 13. november 2007om betalingstjenester i det indre marked og om ændring af direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om ophævelse af direktiv 97/5/EF. (PSD I).

Forslag til rettsakter

Proposal for a directive of the European parliament and of the council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC. (COM(2023) 366 final).

Proposal for a directive of the European parliament and of the council the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849. (COM/2021/423 final).

Proposal for a regulation of the European parliament and of the council payment services in the internal market and amending Regulation (EU) No 1093/2010. (COM(2023) 367 final).

EBA, «Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)», 23. februar 2017. (EBA/RTS/2017/02).

VEILDEDERE, RUNDSKRIV OG UTTALELSER:

European Banking Association

EBA, «Consultation Paper on Draft Guidelines on fraud reporting requirements under Article 96(6) of Directive (EU) 2015/2366 (PSD2)», 2. august 2017. (EBA/CP/2017/13).

EBA, «Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)», 12. desember 2017. (EBA/GL/2017/17).

EBA, «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 ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849», 1. mars 2021. (EBA/GL/2021/02).

EBA, «Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849», 22. november 2022. (EBA/GL/2022/15).

EBA, «Opinion of the European Banking Authority on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2», 29. juni 2017. (EBA/Op/2017/09).

EBA, «Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC», 13. juni 2018. (EBA/Op/2018/04).

EBA, «Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2», 21. juni 2019. (EBA/Op/2019/06).

EBA, «Opinion of the European Banking Authority on 'de-risking'», 5. januar 2022. (EBA/Op/2022/01).

EBA, «Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)», 23. juni 2022. (EBA/Op/2022/06).

EBA, «Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector», 13. juli 2023. (EBA/Op/2023/08).

EBA Single Rulebook, EBA-2018-4032.

EBA Single Rulebook, EBA-2018-4034.

EBA Single Rulebook, EBA-2018-4044.

EBA Single Rulebook, EBA-2018-4090.

EBA Single Rulebook, EBA-2018-4127.

EBA Single Rulebook, EBA-2018-4414.

EBA Single Rulebook, EBA-2018-4440.

EBA Single Rulebook, EBA-2019-4556.

EBA Single Rulebook, EBA-2019-4594.

EBA Single Rulebook, EBA-2019-4702.

EBA Single Rulebook, EBA-2020-5133.

EBA Single Rulebook, EBA-2020-5366.

EBA Single Rulebook, EBA-2020-5367.

EBA Single Rulebook, EBA-2020-5673.

EBA Single Rulebook, EBA-2020-5247.

EBA Single Rulebook, EBA-2021-6245.

Financial Action Task Force

FATF) (2014. Guidance for a risk-based approach: The banking sector. *FATF/OECD, Paris.*

FATF (2010). Global Money Laundering and Terrorist Financing Threat Assessment. *FATF/OECD, Paris*.

FATF (2020a). Guidance on Digital Identity. *FATF, Paris.*

FATF (2020b). Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. *FATF, Paris*.

FATF (2023). Anti-money laundering and counter-terrorist financing measures – Norway, 1st Regular Follow-up Report. *FATF, Paris.*

Øvrige

Basel Committtee on Banking Supervision (Basel) (2001). QIS2 – Operational risk loss data. *Basel*, *QIS survey*. (Basel Committee - QIS 2 - Operational Risk Loss Data – 4 May 2001 (bis.org))

Europeiske sentralbanken (2014). Assessment guide for the security of internet payments. *European Central Bank, Frankfurt am Main*. ISBN: 978-92-899-1159-7.

Europeiske kommisjonen (2022). Opinion No. 3/2022 of the Cooperation Network on the Norwegian eID schemes "Buypass ID" and "BankID".

Finanstilsynet, «Veileder til hvitvaskingsloven», 15. november 2022. (RFT-2022-4).

International Organization for Standardization (ISO) (2018). Risk management – Guidelines. ISO/TC 262. (ISO 31000:2018).

International Organization for Standardization (ISO) (2016). Anti-bribery management systems – Requirements with guidance for use. ISO/TC 309. (ISO 37001:2016)

International Organization for Standardization (ISO) (2013). Risk management – Guidance for the implementation of ISO 31000. ISO/TC 262. (ISO/TR 31004:2013).

International Organization for Standardization (ISO) (2009). Risk management – Terminology. ISO/TC 262. (SN-ISO Guide 73:2009).

International Organization for Standardization (ISO) (2009). Risk management – Risk assessment techniques. ISO/TMBG. (ISO 31010:2009).

PRAKSIS

Høyesterett

Rt. 2001 s. 1006.

Rt. 2010 s. 1445, avsnitt 133.

Rt. 2000 s. 1811.

Rt. 2013 s. 1601.

HR-2020-2021-A.

HR-2022-1752-A.

HR-2022-2468-A.

HR-2023-1850-U.

HR-2017-1037-U.

Underrettspraksis

LF-2014-9728 (Frostating).

LB-2016-20015 (Borgarting).

TSOFT-2017-175325 (Oslo tingrett).

LB-2022-36100 (Borgarting).

LB-2022-74994 (Borgarting).

LE-2022-150063 (Eidsivating).

LB-2023-32107 (Borgarting).

EU-domstolen

Dom av 13. desember 1989, *Grimaldi*, Case C-322/88, EU:C:1989:646.

Dom av 29. april 2004, *Björnekulla.* C-371/02, EU:C:2004:275.

Dom av 19. april 2016, *Ajos,* C-441/14, EU:C:2016:278.

Dom av 16. mars 2023, C-351/21, EU:C:2023:215.

Forvaltningspraksis

Finanstilsynet, «Tilsynsrapport», 28. juni 2021 av Sandnes Sparebank. (20/8370)

Finanstilsynet, «Tilsynsrapport», 12. januar 2021 av Tinn Sparebank. (20/762).

Finanstilsynet, «Tilsynsrapport», 26. september 2022 av Eidsberg Sparebank. (21/668).

Finanstilsynet, «Tilsynsrapport og vedtak om overtredelsesgebyr», 28. oktober 2022 av Santander Consumer Bank AS. (21/6151).

Finanstilsynet, «Tilsynsrapport», 19. desember 2022 av Nordea Bank Adp. (20/4183).

Finanstilsynet, «Tilsynsrapport», 20. mars 2023 av Sparebanken Møre. (21/395).

Finansinspektionen, «Order of correction», 25. juni 2020 av Skandinviska Enskilda Banken AB (SEB). (SEB AB 25.06.2020).

Forbrukertilsynet, «Orientering til bankene - krav til bankenes tilbakeføring av forbrukers tap ved uautoriserte transaksjoner», 1. desember 2022, Nr. 22/4043-44, s. 7.

Finansklagenemnda

BKN-2007-15.

FinKN-2018-305.

Finkn-2019-39.

Finkn-2019-40.

Finkn-2019-939.

FinKN-2020-703.

FinKN-2020-706.

FinKN-2020-707.

FinKN-2020-897.

FinKN-2020-963.

FinKN-2020-973.

Finkn-2020-355.

Finkn-2020-455.

Finkn-2021-32.

FinKN-2021-36.

Finkn-2021-107.

Finkn-2021-224.

Finkn-2021-426.

Finkn-2021-792.

Finkn-2021-838.

Finkn-2021-1110.

Finkn-2021-1262.

FinKN-2023-31.

Finkn-2023-592.

STANDARDAVTALER:

Bits (2019). Avtalevilkår for PersonBankID og AnsattBankID – PDS. BankID PKI Disclosure Statement. Ver 1.1. (21.05.2019), godkjent av BankID Policy Board den 21.05.2019.

Bits (2021). Vedlegg 1 til Regler for avregning og oppgjør av transaksjoner som inngår i Norwegian Interbank Clearing System (NICS). Sist oppdatert av Bits AS 03.02.2021, med ikrafttredelse 22.04.2021.

Bits (2023a). Regler for avregning og oppgjør av transaksjoner som inngår i Norwegian Interbank Clearing System (NICS). Fastsatt av styret i NICS Operatørkontor 06.07.2010 etter behandling i Bransjestyre bank og betalingsformidling i Finansnæringens Fellesorganisasjon (FNO) den 05.07.2010. Endret av Bits AS 10.12.2019 og oppdatert 08.02.2022 som følge av utfasing av Straks 1.0. Sist oppdatert 14.02.2023 med mindre justeringer for å ivareta krisehåndteringsregler (NICS-reglene-oppdatert-14.02.2023.pdf (bits.no).

Bits (2023b). Regler om straksbetalinger med sikkert oppgjør. Fastsatt av Bits AS 28.11.2019. Ikrafttredelse 06.01.2020. Endret av Bits AS 14.02.2023 (https://www.bits.no/document/regler-om-straksbetalinger-med-sikkert-oppgjor-endret-14-02-2023-3/).

Lending Standards Board (2023). Contingent Reimbursement Model Code for APP scams (the CRM Code).

LITTERATUR:

Bøker

Amir Habibija, «Tapsfordeling mellom bank og kunde ved misbruk av elektroniske betalingsinstrumenter», i *Bruk og misbruk av elektronisk identifikasjon*, Marte Eidsand Kjørven, Maria Astrup Hjort og Tone Linn Wærstad (red.), Karnov forlag 2022.

Neergaard, Ulla, Ruth Nielsen (2021). EU-ret (8. utgave.). Karnov Group, s. 113.

Rui, Jon Petter (2012). Hvitvasking: Fenomenet, Regelverket, Nye Strategier. *Universitetsforlaget, Oslo*.

Rui, Jon Petter, Gunnar Holm Ringen, Kristine Frivold Rørholt (2022). *Hvitvaskinngsloven – Ajourført lovkommentar.* Juridika.

Artikler, rapporter og meldinger

Aleroud, Ahmed, Lina Zhou (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, Volume 68, 160-196. ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.04.006.

Aven, Terje (2013). On the meaning and use of the risk appetite concept. *Risk analysis*, 33(3), 462-468. https://doi.org/10.1111/j.1539-6924.2012.01887.x.

Brombach, Harald, «Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap», *Digi.no*, 24. februar 2022 (https://www.digi.no/artikler/skadevare-viser-at-angrepet-pa-ukraina-har-vaert-forberedt-i-flere-maneder/517579, lest 7. november 2023).

Chau, D., & van Dijck Nemcsik, M. (2020). *Anti-Money Laundering Transaction Monitoring Systems Implementation: Finding Anomalies.* John Wiley & Sons.

Conti, M., Dragoni, N., og Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18(3), 2027-2051.

Den Europeiske kommisjonen (2023). Commission staff working group dokument impact assessment report. *Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Brussels.* (SWD 2023/231 final).

DNB v/Financial Cyber Crime Center (FCR) (2022). Annual Fraud Report. *DNB/FCR, Oslo.*

DNB, Antihvitvasking, antikorrupsjon og internasjonale sanksjoner. (https://www.dnb.no/om-oss/barekraft/mal-og-ambisjoner/okonomisk-kriminalitet/anti-hvitvasking-og-bekjempelse-av-terrorfinansiering, lest 7. november 2023).

EU (2023). Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (2023/C 237/06). *Official Journal of the European Union, C 237/6*.

European Banking Association (EBA) (2016). Public Hearing on strong customer authentication & secure communication (SCA & CSC) under Aricle 97 PSD2. *EBA offices, London*, s. 19. (https://www.eba.europa.eu/sites/default/documents/files/document_library/Calendar/Public%20Hearings/2021/Public%20hearing%20on%20the%20Consultation%20paper%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC%20under%20PSD2/1023889/Public%20hearing%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC%20with%20respect%20to%20the%2090-days%20exemption%20for%20account%20access.pdf)

Europeiske kommisjonen (2020). Meddelelse fra kommisjonen om en handlingsplan for en samlet EU-politik for forebyggelse af hvidvaskning af penge og finansiering af terrorisme. *Den Europæiske Unions Tidende, Brussels* (2020/C 164/06).

Europeiske parlamentet (2023). Ordinary legislative procedure (ex-codecision procedure) Regulation Amending Regulation 2010/1093 2009/0142(COD) 23. August 2023, Payment services in the internal marked (2023/0210(COD)). (https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/0210(COD)&l=en, sist lest 7. november 2023).

Europeiske sentralbanken (2018). Fifth report on card fraud. *European Central Bank, Frankfurt am Main*. ISSN 2315-0033, DOI:10.2866/333885. (https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport201809.en.pdf).

Europol (2021). European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime. *Publications Office of the European Union, Luxembourg*.

Feratovic, Leila, «ID-svindel: Sikkerhetsekspert kritiserer bankene», *E24*, 2. februar 2020 (ID-svindel: Sikkerhetsekspert kritiserer bankene – E24, lest 7. november 2023).

Finanstilsynet (2023). Risiko- og sårbarhetsanalyse (ROS). *Finanstilsynet, Oslo*.

Finanstilsynet, «Retningslinjer frå EBA om kundeetablering utan personleg oppmøte trer i kraft 2. oktober 2023», nyhetsmelding 23. juni 2023. (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2023/retningslinjer-fra-eba-om-kundeetablering-utan-personleg-oppmote-trer-i-kraft-2.-oktober-2023, sist lest 7. november 2023).

Finanstilsynet, «Sterk kundeautentisering under PSD 2», nyhetsmelding 21. juni 2019. (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2019/sterk-kundeautentisering-under-psd2/, sist lest 7. november 2023).

Finanstilsynet, «Unntak fra sterk kundeautentisering», nyhetsmelding 22. april 2022. (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2022/unntak-fra-sterk-kundeautentisering/, sist lest 7. november 2023).

Finanstilsynet, «Uttale frå EBA om risikoen for kvitvasking og terrorfinansiering», nyhetsmelding 9. august 2023. (https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2023/uttale-fra-eba-om-risikoen-for-kvitvasking-og-terrorfinansiering/, sist lest 7. november 2023).

Foley, Linda, Jay Foley (2003). Identity theft: The aftermath 2003. San Diego, CA: Identity Theft Resource Center: Litan, A.(2007). *The truth behind identity theft numbers.* Gartner Research Group: Stamford, CT.

Gontarek, Walter, Ruth Bender (2019). Examining risk governance practices in global financial institutions: the adoption of risk appetite statements. *Journal of Banking Regulation*, 20, 74-85. https://doi.org/10.1057/s41261-018-0067-2.

Hertzberg, Ingrid, Tarjei Bekkedal (2018). Kompetanse uten kontroll? Om Norges tilslutning til EUs finansbyråer (II). *Lov og rett*, 57(4), 205–226. https://doi.org/10.18261/issn.1504-3061-2018-04-03.

Kjørven, Marte Eidsand., Alf Petter Høgberg, Geir Woxholth (2021). BankID-opplysninger på avveie – om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 (3) og ny finansavtalelov § 4-30 (4). Lov og rett, 60(6), s. 335–366. https://doi.org/10.18261/issn.1504-3061-2021-06-03.

Levine, Ross (2004). The corporate governance of banks: A concise discussion of concepts and evidence. Vol. 3404. *World Bank Publications, USA.*

Marasa, Flaminia (2020). The Processing of Personal Data of Payment Service Users between PSD2 and GDPR. *Orizzonti del Diritto Commerciale*, s. 629.

Meld. St. 18 (2022–2023) Finansmarkedsmeldingen 2023.

Norges Bank (2022). Det norske finansielle systemet 2022. *Norges Bank, Oslo.* ISSN 2535-3993.

Norsk senter for informasjonssikring (NorSIS) (2023). Nordmenn og digital sikkerhetskultur 2023. *NorSIS, Oslo*.

Norum, Halvar, Marthe Knudsen, «Får gigant-bot og ramsalt kritikk av Finanstilsynet», *Aftenposten*, 3. mai 2021 (oppdatert 15. september 2021) (https://www.nrk.no/norge/dnb-far-400-millioner-kroner-i-gebyr-av-finanstilsynet-for-manglende-oppfolging-av-hvitvaskingsloven-1.15479891, lest 7. november 2023).

Ofoeda, Joshua, Richard Boateng, John Effah (2019). Application programming interface (API) research: A review of the past to inform the future. *International Journal of Enterprise Information Systems (IJEIS),* 15.3, s. 76-95. https://doi.org/10.4018/ijeis.2019070105.

Økokrim (2022). Trusselvurdering 2022. *Økokrim, Oslo*, s. 49.

Økokrim (2023a). Bedrageri – et samfunnsproblem. *Økokrim, Oslo.*

Økokrim (2023b). Årsrapport 2022. *Økokrim, Oslo*.

Økokrim v/Enheten for finansiell etterretning (EFE) (2023). Årsrapport 2022. *Økokrim/FUI, Oslo*, s. 10.

Oo, Kyaw Zay (2019). Design and implementation of electronic payment gateway for secure online payment system. *Journal of Trend in Scientific Research and Development (ijtsrd),* Volum 3.5, 1329-1334. ISSN: 2456-6470 https://doi.org/10.31142/ijtsrd26635.

Polismyndigheten (2022). De dödliga bedrägerierna. *Polismyndigheten/Nationella operativa avdelningen/Nationellt Bedrägericentrum, Stockholm*, s. 21.

Politiet v/Kripos (2023). Cyberkriminalitet 2023. *Politiet/Kripos, Oslo*.

Puschmann, Thomas (2017). Fintech. *Business & Information Systems Engineering*, 59, 69-76.

Romanova, Inna, et al. (2018). The payment services Directive II and competitiveness: The perspective of European fintech companies. *European Research Studies,* 21.2, 3-22.

Rui, Jon Petter (2023). Om bankers rett til avslag/oppsigelse og plikt til avvisning og avvikling av kundeforhold grunnet i hvitvaskingsloven. *Tidsskrift for forretningsjus*, 29(1), 2–49. https://doi.org/10.18261/tff.29.1.1.

Sharif-Askary, Ahmed K. Elmagarmid Jamshid (1992). Reservable Transactions: An Approach for Reliable Multidatabase Transaction Management. *Department of Computer Science Technical Reports.* Paper 937. (https://docs.lib.purdue.edu/cstech/937).

Sheedy, Elizabeth, Le Zhang, Kenny Chi Ho Tam (2019). Incentives and culture in risk compliance, *Journal of Banking & Finance*, Volume 107, 105611. https://doi.org/10.1016/j.jbankfin.2019.105611.

Skatteetaten (2021). Trusselvurdering Covid-19. *Skatteetaten*.

Stulz, R.M. (2015). Risk-Taking and Risk Management by Banks. *Journal of Applied Corporate Finance*, 27, s. 8-18. https://doi.org/10.1111/jacf.12099.

Svigghum, Silje Kathrine, Emma Fondenes Øvrebø, Ola Haram, Silje Lien Sveen, Ingvill Dybfest Dahl, «BankID og Arbeidstilsynets nettsider er nede - ustabilitet i Altinn», *e24*, 29. juni 2022 (https://e24.no/naeringsliv/i/7d2Gvv/bankid-og-arbeidstilsynets-nettsider-er-nede-ustabilitet-i-altinn, lest 7. november 2023).

Torset, Nina Selbo, «Stor avsløring: Swedbank anklages for storstilt hvitvasking», *Aftenposten*, 20. februar 2019 (https://www.aftenposten.no/okonomi/i/ddV5zj/stor-avsloering-swedbank-anklages-for-storstilt-hvitvasking , lest 7. november 2023).

Wood, Helena, Tom Keatinge, Keith Ditcham, og Ardi Janjeva (2021). The silent threat: the impact of fraud on UK national security. *RUSI Occasional Paper*, January.

Yeboah-Boateng, E.O. and Amanor, P.M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5(4)*, s. 297-307.

Zachariadis, Markos, Pinar Ozcan (2017). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. *SWIFT Institute Working Paper* No. 2016-001. http://dx.doi.org/10.2139/ssrn.2975199.