NTAES

Nyere betalingstjenester

GRUNNLAGSDOKUMENT

Nasjonalt tverretatlig analyse- og etterretningssenter

Publikasjonens tittel: Nyere betalingstjenester - Grunnlagsdokument
Utgitt: juni 2017
Utgitt av: Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
Kontakt: post@ntaes.no
Postadresse: c/o ØKOKRIM, Postboks 8193 Dep, N-0034 Oslo
Besøksadresse: C.J. Hambros plass 2, 0164 Oslo

Illustrasjoner: Shutterstock
Grafisk design: ØKOKRIM

Forord

Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) startet opp 2. mai 2016 og er et av tiltakene i Regjeringens strategi mot arbeidslivskriminalitet fra 13. januar 2015.

Formålet til senteret er å legge til rette for at politi- og kontrolletatene bedre kan utnytte den samlede analyse- og etterretningsinformasjon etatene besitter. Senteret skal utarbeide kunnskapsbasert grunnlag for politiets og kontrolletatenes egne og felles tverretatlige prioriteringer. Dette skal bidra til å utvikle og gjennomføre en mer målrettet, effektiv, slagkraftig og treffsikker bekjempelse av økonomisk kriminalitet, herunder arbeidslivskriminalitet.

Hovedoppdraget er å utarbeide nasjonale trussel- og risikovurderinger som grunnlag for strategiske beslutninger om tiltak innen økonomisk kriminalitet, herunder arbeidslivskriminalitet. Senteret skal også utarbeide etterretningsprodukter som gir grunnlag for innsats mot kriminalitet.

Det sentrale samarbeidsforum (DSSF) som består av riksadvokaten, politidirektøren, sjef ØKOKRIM, skattedirektøren, tolldirektøren, NAV-direktøren og direktøren for Arbeidstilsynet gir senteret føringer og beslutter dets oppdrag.

Et av oppdragene til NTAES er å foreta en kartlegging av nyere betalingstjenester og deres sporbarhet, og vurdere hvordan manglende sporbarhet utgjør en trussel for etatenes arbeid i bekjempelsen av økonomisk kriminalitet.[1]

Med digitalisering av økonomien, teknologisk utvikling og deregulering av finansmarkedene i EU, følger fremveksten av ulike nye betalingstjenester. De nye betalingstjenestene etterlater seg en rekke elektroniske spor. Dessverre er mange av disse sporene i liten grad tilgjengelig for etatene.

Dokumentet beskriver nyere betalingstjenester og etatenes erfaringer og utfordringer.

Vurderingen av hvordan nyere betalingstjenester utgjør en trussel for etatenes arbeid med bekjempelse av økonomisk kriminalitet er beskrevet i en separat rapport.[2]

[1] Med *manglende sporbarhet* menes at spor av transaksjonen enten ikke finnes, eller at sporene er utilgjengelig for etatene ved at det er lagret i et uleselig/uforståelig dataformat, eller at etatene ikke har nødvendige hjemler for å hente de inn. Med *spor* menes data om transaksjonen som gjør det mulig å identifisere hvem som er mottaker og/eller avsender av transaksjonen, enten direkte eller indirekte.
[2] Nasjonalt tverretatlig analyse og etterretningssenter (NTAES) – Trusselvurdering Nyere betalingstjenester

Innholdsfortegnelse

Forord ... 3
Innledning ... 6
Sammendrag ... 7
Metode ... 8
Kapittel 1 Beskrivelse av nyere betalingstjenester ... 9
Definisjon nyere betalingstjenester ... 9
Drivere i utviklingen av nyere betalingstjenester ... 10
Regulatorisk rammeverk ... 11
Forhåndsbetalte kort ... 12
Open Loop ... 12
Closed loop og restricted loop ... 14
Personlig/ikke personlig ... 14
Ladbart/ikke ladbart ... 14
Internettbaserte betalingstjenester ... 15
Struktur/ mekanismer ... 15
Betalingsformidler ... 15
Tredjepartstilbyder ... 16
E-wallet ... 16
Cash voucher/e-voucher ... 17
Faktura ... 18
Mobile betalingstjenester ... 18
Mobil wallet, telefaktura og mobile tredjepartstilbydere ... 18
Betalingsformidler ... 20
Virtuell valuta ... 21
Kategorier ... 21
Struktur ... 22
Kryptovaluta ... 22
Viktige funksjoner ... 25
Viktige roller i omsetning og bruk av virtuelle valutaer ... 25
Skattemessige konsekvenser ... 26
Trender ... 26
Økt konkurranse på markedet ... 26
Virtuelle valutaer ... 27
Nettsedler ... 28
Kapittel 2: Nyere betalingstjenester og sporbarhet ... 29
Hvilke spor legger nyere betalingstjenester ... 29

Forhåndsbetalte kort 29
Internettbaserte betalingstjenester 30
Mobile betalingstjenester 33
Virtuell valuta 33
Hvilke hindre står kontrolletatene overfor 34
Kryptering 34
Mellomtjenere og Virtuelle Private Nettverk (VPN) 34
Darkweb, Darknet og Tor-nettleser 35
Kapittel 3: Bruk av nyere betalingstjenester ved utøvelse av økonomisk kriminalitet 37
Drivere 37
Omfang 38
Saker med virtuell valuta 38
Saker med internettbaserte betalingstjenester 39
Saker med forhåndsbetalte kort 40
Saker med mobile betalingstjenester 41
Kapittel 4: Politi- og kontrolletatenes erfaringer med nyere betalingstjenester 42
Etatenes forhold til nyere betalingstjenester 42
Nærmere om etatenes erfaringer 45
Arbeidstilsynet 45
NAV Kontroll 45
Tolletaten 45
Skatteetaten 46
Politiet 48
Felles problem, ulike utfordringer 50
Vedlegg 1 Begrepsforklaringer 52
Vedlegg 2 Regelverk 54
Betalingstjenestedirektiv nr. 1 (PSD – Payment Service Directive) 54
Betalingstjenestedirektiv nr. 2 (PSD2-Payment service directive 2) 55
Rettslig vurdering av elektroniske penger (E-penger) 56
Finanstilsynets rolle 59
Hvitvaskingsregelverket 62
Rapporteringsplikt til valutaregisteret 65
Utveksling av finansielle kontoopplysninger etter FATCA og CRS 67

Innledning

Grunnlagsdokumentet som er utarbeidet av NTAES er en kartlegging av nyere betalingstjenester og deres sporbarhet. Dokumentet er et kunnskapsprodukt om nyere betalingstjenester og beskriver utfordringer etatene har med sporing av transaksjoner.

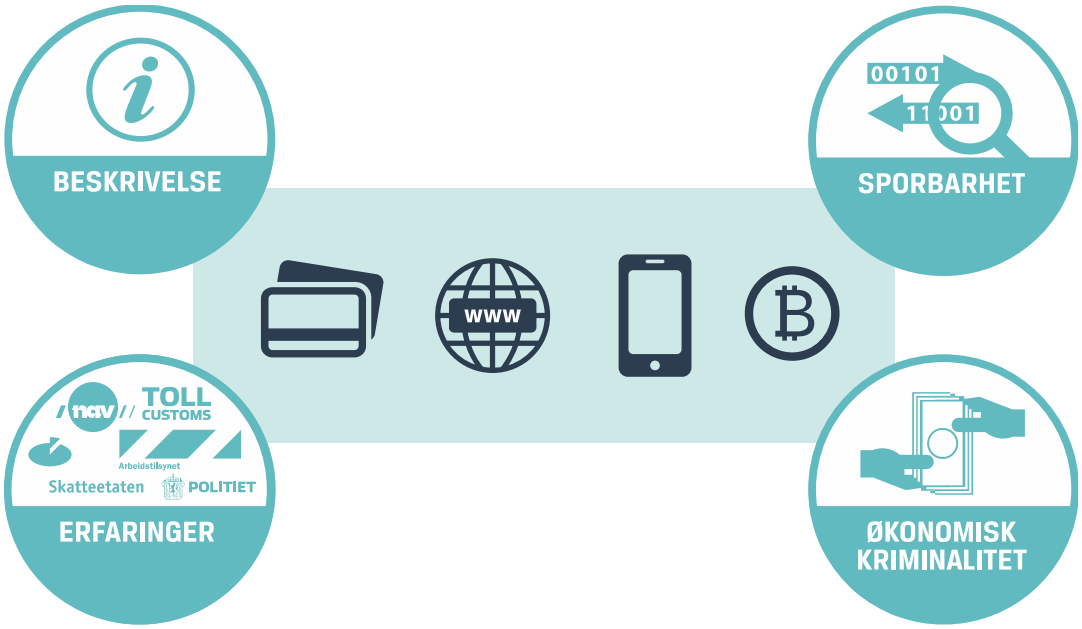
Dokumentet er grunnlaget for trusselvurderingen.[3] Trusselvurderingen er et separat dokument for Det sentrale samarbeidsforum (DSSF) og er utarbeidet for å gi et felles grunnlag til politi- og kontrolletatene for å vurdere hvilken trussel de nyere betalingstjenestene og manglende sporbarhet representerer.

NTAES har delt nyere betalingstjenester inn i følgende kategorier:

- Forhåndsbetalte kort
- Internettbaserte betalingstjenester
- Mobile betalingstjenester
- Virtuelle valutaer

NTAES har brukt økonomisk kriminalitet som ramme i oppdraget.[4] Transaksjoner med bruk av nyere betalingstjenester benyttes åpenbart også innen annen profittmotivert kriminalitet, som for eksempel narkotikakriminalitet og cyberkriminalitet.

Grunnlagsdokumentet inneholder en beskrivelse av nyere betalingstjenester, tjenestenes sporbarhet, bruk av nyere betalingstjenester innen økonomisk kriminalitet og politi- og kontrolletatenes erfaringer med nyere betalingstjenester.



[3] Nasjonalt tverretatlig analyse og etterretningssenter (NTAES) – Trusselvurdering Nyere betalingstjenester

[4] Økonomisk kriminalitet er profittmotiverte, lovstridige handlinger som ofte begås innenfor eller med utspring i en økonomisk virksomhet som i seg selv er – eller gir seg ut for å være – lovlig. (www.okokrim.no)

Sammendrag

Nyere betalingstjenester har utviklet seg forskjellig fra land til land. Årsaken er ulike forutsetninger knyttet til for eksempel økonomiske forhold og befolkningens bruk av teknologi. EU har gjennom direktiver lagt til rette for større konkurranse i markedet for betalinger for å gjøre betalingssystemet billigere og raskere, både internt i enkelte land og på tvers av landegrensene.

Med forhåndsbetalte kort kan kunden være anonym dersom kunden holder bruken under angitte beløpsgrenser. I utlandet kan det anskaffes kort med høye beløpsbegrensninger som ikke krever at kunden legitimerer seg. Slike kort er som regel knyttet til Visa eller Mastercard og kan dermed benyttes over hele verden samt kombineres med de fleste andre nyere betalingstjenester. Straffesaker i Norge har vist at forhåndsbetalte kort benyttes til å skjule midler fra straffbare handlinger.

Internettbaserte betalingstjenester er vurdert til å være betalingsformidlere, tredjepartstilbydere, e-wallets, vouchers og faktureringstjenester. Både betalingsformidlere og e-wallets har interne kontoløsninger. Vouchers kan kjøpes anonymt, noe som vanskeliggjør sporing av transaksjoner. Eksempler fra straffesaker viser at slike løsninger er brukt til å føre penger ut av landet.

Mobile betalingstjenester i Norge er per i dag kun knyttet til norske kort og konti. Det er foreløpig ikke mulig å gjennomføre grensekryssende transaksjoner med slike tjenester. Det er derfor lav risiko knyttet til manglende sporbarhet for tjenestene. Straffesaker omhandler mindre bedragerier og kjøp og salg av ulovlige varer. Etatene har lite erfaring med mobile betalingstjenester.

Kryptovalutaer er den av de virtuelle valutaene som best egner seg til å skjule spor. Bruken er anonym og kunder kan overføre til hvor som helst i verden. Kjøp av kryptovaluta kan gjøres helt anonymt. Mange kryptovalutaer øker i markedsverdi, men Bitcoin er fortsatt størst. Etatenes erfaringer er særlig knyttet til Bitcoin. Den stadig økende bruken, utbredelsen og kunnskapen om kryptovalutaene øker risikoen for at de blir benyttet til å skjule spor knyttet til utbytte av kriminalitet.

Politi- og kontrolletatenes erfaringer med nyere betalingstjenester er ulik. Etatene har ulike forutsetninger for å følge spor etter bruk av nyere betalingstjenester, ulik kompetanse på området og ulike muligheter for innhenting av opplysninger fra tilbydere i utlandet.

Metode

Metodikken til NTAES er basert på politiets etterretningsdoktrine.[5]

Innhentingsprosessen ble innledet med utgangspunkt i tre prioriterte etterretningsbehov (PEB) for oppdraget:

1. Gjør bruk av nyere betalingstjenester det enklere å skjule økonomisk kriminalitet?
2. Er bruk av nyere betalingstjenester økende i omfang?
3. Har etatene tilstrekkelig kunnskap om nyere betalingstjenester?

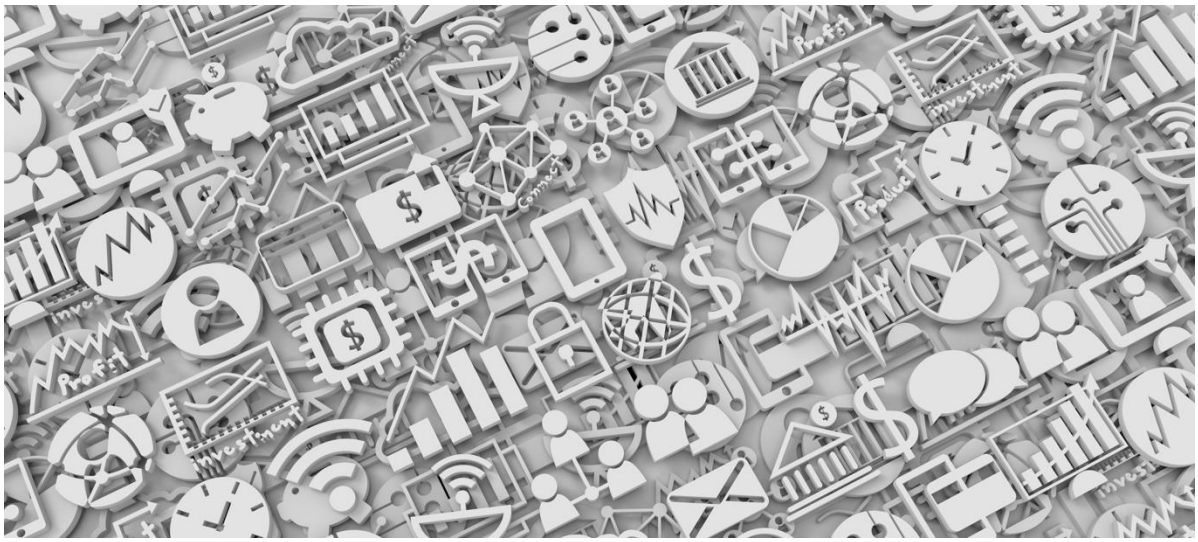
Informasjonsbehov for å svare ut prioriterte etterretningsbehov, og relevante kilder er kartlagt i en innhentingsplan.

Både kvantitative og kvalitative metoder er benyttet for innhenting. Det er gjennomført intervjuer, presentasjoner basert på spørsmål fra NTAES, uttrekk fra valutaregisteret, analyse av relevante straffesaksdokumenter og dommer, søk i åpne kilder herunder offentlige rapporter og avisartikler, og innhentet erfaringer fra etatene gjennom spørreskjema til aktuelle miljøer. Bakgrunnsinformasjon er også hentet fra betalingsformidlingsbransjen gjennom blant annet Betalingsformidlingskonferansen 2016 og FutureBank 2017 i regi av Finans Norge.

Det er under arbeidet konsultert med:

- Finanstilsynet
- Bits AS
- ØKOKRIM
- Kripos
- Øko-team i politiet
- Skatteetaten
- Tolletaten
- NAV Kontroll
- Arbeidstilsynet

[5] Etterretningsdoktrine for politiet, 2014



Kapittel 1 Beskrivelse av nyere betalingstjenester

Definisjon nyere betalingstjenester

Financial Action Task Force (FATF) sin definisjon av nyere betalingstjenester er:[6] *"Nyere betalingstjenester anses å være nye og innovative betalingsprodukter og tjenester som tilbyr et alternativ til tradisjonelle finansielle tjenester. Nyere betalingstjenester inkluderer en rekke produkter og tjenester som involverer nye måter å initiere betalinger gjennom eller utvide rekkevidden til tradisjonell elektronisk handel, samt produkter som ikke baserer seg på tradisjonelle systemer for å overføre en verdi mellom enkeltpersoner eller organisasjoner."*[7]

Betalingssystemet har i de senere årene blitt segmentert og spesialisert. Dette har resultert i at tjenesteleverandører som ikke er banker konkurrerer i markedet for godkjenning av transaksjoner. Slike nye aktører har kunnet tilpasse betalingsinstrumentene og pakke dem med produkter spesialsydd for det ønskede marked. Transaksjoner utføres, databaser vedlikeholdes og det opereres som verdileverandør i e-pengeordninger. Slike tjenester betegnes i grunnlagsdokumentet som nyere betalingstjenester.

[6] Financial Action Task Force (FATF) er et organ bestående av 35 medlemsland og som setter internasjonale standarder for hvitvasking og terrorfinansiering, www.fatf-gafi.org FATF members
[7] FATF Guidance for a risk based approach: Prepaid cards, Mobile payments and internet-based payment services, 2013 (side 4)

Drivere i utviklingen av nyere betalingstjenester

Det er flere årsaker til fremveksten av nyere betalingsmetoder. Blant annet er følgende faktorer forskjellig fra land til land:[8]

- Politikk
- Reguleringer
- Teknologi
- Lokale preferanser
- Kostnader
- Økonomiske forhold
- Nasjoners og private selskapers påvirkning på betalingssystemet

Driverne i utviklingen av nyere betalingstjenester er ofte en blanding av utforming av nåværende betalingssystemer, internasjonale og nasjonale ønsker om mer konkurranse samt forbrukeres og næringslivets forventninger.[9]

Nyere betalingstjenester er innrettet for å være raskere, billigere og enklere i bruk enn en tradisjonell internasjonal banktransaksjon. I takt med at det stadig lanseres nye betalingstjenester øker forbrukernes forventninger til hele brukeropplevelsen rundt betalingen. Den teknologiske utviklingen på området har foretatt et stort sprang og kundene har blitt vant med løsningene.[10] Det forventes at tjenesten skal være lett tilgjengelig, gjerne i en mobilapplikasjon. I tillegg skal betalingene skje raskt, være billige og sikre.[11]

Forhandlere er opptatt av forbrukernes behov, og beskriver at det er viktig å holde på kundene gjennom betalingsprosessen. Forhandlere tilbyr derfor et utvalg av betalingsløsninger som er mobiltilpassede, innbydende og enkle for kundene.[12]

EU har vært en pådriver for et felles betalingsmarked. Som en del av dette har det blitt utarbeidet direktiver som både legger til rette for og regulerer betalingstjenester som kan redusere kostnader, tidsbruk og øke konkurransen både internt i det enkelte land men også på tvers av landegrenser.

Utviklingen av nyere betalingstjenester varierer regionalt og fra land til land ettersom forutsetningene er forskjellige. I land uten et utbredt banksystem, eksempelvis i Kenya, er mobilbetalinger størst, der teleoperatøren står for banktilknytningen.

[8] FATF Report on new payment Methods, 2006 (Side 2)
[9] PWC Emerging markets driving the payments transformation (Side 3)
[10] www.Evry.com Open banking a transformational opportunity for banks
[11] Dibs Norsk E-handel 2016 (Side 34, 35 og 41)
[12] Dibs Norsk E-handel 2016 (Side 41)

Regulatorisk rammeverk

I det regulatoriske rammeverket som tilbyderne opererer innenfor, er følgende sentrale i rapporten:

- Nye betalingstjenesters tilgang til markedet, og regulering av disse gjennom det første betalingstjenestedirektivet fra 2007.[13]
- Økt konkurranse og flere nye betalingstjenesters tilgang til markedet gjennom det andre betalingstjenestedirektivet (PSD2) fra 2018.[14]
- Felles e-pengeregulering i EU og nye aktørers tilgang til markedet gjennom e-pengedirektivet fra 2009.[15] Regler om e-penger i finansforetaksloven er bygget på direktivet.[16]
- Finanstilsynets rolle med å gi konsesjon og føre tilsyn med aktører som tilbyr nye betalingstjenester i Norge, og deres begrensede mandat overfor aktører som melder om grensekryssende virksomhet til Norge.[17]
- Plikt til å foreta kundekontroll og unntak fra denne som følger av hvitvaskingsloven.[18] Tersklene for krav til identifikasjon og legitimasjon ved utstedelse av elektroniske penger er gitt her.[19] Ved beløp på mer enn 250 Euro må brukeren gi opplysninger ved opprettelse av konto, og det er krav om legitimasjon. Er beløpet *lavere* enn 250 Euro, står rapporteringspliktige fritt, og kan unnta fra kundekontroll (det vil si la brukeren være anonym).
- I forslag til endringer i 4. hvitvaskingsdirektiv foreslås å redusere grensen fra krav til identifikasjon fra 250 til 150 Euro, samtidig som krav til kundekontroll utvides. Videre foreslås at forhåndsbetalte kort utstedt utenfor EU bare skal kunne brukes i EU når disse oppfyller krav som svarer til 4. hvitvaskingsdirektiv.[20]
- Rapporteringsplikt for mistenkelige transaksjoner som følger av hvitvaskingsloven.[21]
- I forslag til endringer i 4. hvitvaskingsdirektiv foreslås også at tilbydere av vekslingstjenester mellom virtuelle penger og fysiske penger, såkalte wallet-providers skal omfattes av direktivet og dermed gjøres rapporteringspliktige etter hvitvaskingsregelverket.[22]
- Rapporteringsplikt til valutaregisteret for valutaveksling og overføringer av betalingsmidler inn og ut av Norge for foretak som kan drive valutavirksomhet.[23] Hvem som er rapporteringspliktige til valutaregisteret følger av valutaregisterloven § 4.[24] På oppdrag fra Finansdepartementet er det satt i gang et lovarbeid i Skattedirektoratet som blant annet skal vurdere om ordlyden i

[13] Europa.eu – Direktiv 2007/64/EF – Om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om opphevelse av direktiv 97/5/EF.
[14] *Les mer om PSD2 under* Trender, Betalingstjenestedirektiv nummer 2 *senere i kapittel 1*
[15] E-penge-direktivet 2009/110/EF
[16] Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern
[17] Lov 7. desember 1956 nr. 1 om tilsyn med finansforetak mv. Finanstilsynsloven § 1
[18] Lov 6. mars 2009 nr. 11 om tiltak mot hvitvasking og terrorfinansiering mv.
[19] Hvitvaskingsforskriften § 10, jf. hvvl. § 13
[20] Økonominytt fra EU-delegasjonen, Nr. 2 – Februar 2017
[21] Hvvl. §§ 17 og 18
[22] Wallet-providers er leverandører av digitale lommebøker som gir tilgang til virtuelle penger
[23] Banker, betalingsforetak, e-pengeforetak og finansieringsforetak som har tillatelse til å drive valutavirksomhet, jf. Finansforetaksloven § 2-5 (1)
[24] Lov 28. mai 2004 nr. 29 om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge (valutaregisterloven) § 1

valutaregisterloven § 4 bør endres for å fange opp aktører som faller utenfor regelverket, men som bør være omfattet av rapporteringsplikten.[25]

- Norge har, som ett av 100 land, forpliktet seg til gjensidig automatisk utveksling av finansielle konto-opplysninger etter OECDs nye internasjonale standard, kjent som "the Common Reporting Standard" (CRS).[26] Norge har tolket avtalen slik at e-pengeforetak og andre som utsteder e-penger vil være rapporteringspliktige for kunders beholdning av e-penger, så lenge ikke vilkårene for forenklet kundekontroll er tilstede.[27] Dersom andre land tolker avtalen på tilsvarende måte kan norske skattemyndigheter motta opplysninger om norske kunders beholdninger i e-penger fra store deler av verden.

Regelverket er nærmere redegjort i vedlegg 2.

I resten av kapittel 1 forklares det hvordan de forskjellige typene betalingstjenestene fungerer. I tillegg presenteres noen eksempler på tjenestetilbydere. Avslutningsvis presenteres trender innen betalinger.

Forhåndsbetalte kort

Forhåndsbetalte betalingskort kom på markedet i slutten av 1990-tallet som et alternativ til kreditt-kort og debetkort.[28] Kredittkortselskaper setter krav til kundens kredittverdighet ved utstedelse av kredittkort. Bankkonto kreves for å få debetkort. Det er ikke tilsvarende krav ved utstedelse av forhåndsbetalt kort. I motsetning til et debetkort og kredittkort kan brukeren kun benytte det som er betalt inn på forhånd til kortet. Den forhåndsbetalte verdien oppbevares enten på en konto kun knyttet til det enkelte kort, alternativt kan de være knyttet til en felles konto for alle kortene kortutsteder har. Forhåndsbetalte kort av type Visa eller Mastercard tilbys over hele verden og kan stort sett benyttes på alle brukersteder som godtar Visa eller Mastercard. Kunden kan dermed handle over disk, på nett, foreta kontantuttak, fylle opp e-wallet og så videre.

De forhåndsbetalte kortene har forskjellig funksjonalitet og begrensninger. Under fremgår de forskjellige typene forhåndsbetalte kort.[29]

Open Loop

Open loop kort har mange av de samme funksjonalitetene som et vanlig bankkort. Dette er gjerne Visa eller Mastercard som kan benyttes på nett og i butikker uten de begrensningene som et closed loop kort har. Eksempler på kort som selges i Norge er SpendOn, Easipay og Paygoo (se faktabokser). Eksempel på et utenlandsk kort som ikke selges i Norge er Swiss bankers (se faktaboks). Kortene er regnet som e-penger.

[25] Ref. oppdragsbrev fra Finansdepartementet av 16. februar 2017, Del 1, punkt 2
[26] Oversikt over hvilke land som har inngått CRS-avtale fremgår av https://www.oecd.org CRS by jurisdiction
[27] Vilkårene for forenklet kundekontroll følger av hvitvaskingsforskriften § 10
[28] FATF Guidance for a risk based approach Prepaid cards, Mobile payments and internet-based payment services, 2013 (Side 5)
[29] FATF Guidance for a risk based approach Prepaid cards, Mobile payments and internet-based payment services, 2013 (Side 5)

SpendOn
SpendOn Visa utstedes av Sparebank 1 SMN Card Solutions AS. SpendOn VISA gavekort er et ikke-ladbart forhåndsbetalt kort. SpendOn ble lansert i 2008. Privatpersoner kan velge mellom 500 eller 1000 kroner, mens bedriftskunder kan velge opp til 5 000 kroner. Det fås kjøpt hos Rema 1000. Kortet er upersonlig og kan benyttes til online kjøp og til kjøp hos forhandlere som aksepterer Visa, men kan ikke benyttes til kontantuttak.

Easipay
Easipay kortet er utstedt av IDT Financial Services Limited, som er regulert som bank og har hovedkontor på Gibraltar. De tilbyr et forhåndsbetalt kort knyttet til Mastercard som kan lades. Det er forskjellige måter å fylle opp kortet på, nettbank, mobilbank, giro, Paysafecard verdivoucher eller Vipps. Det er mulig å betale fakturaer med kortet, og kortet kan benyttes til å motta lønn. Ifølge easipaycard.no er Easipay-konto en e-pengekonto som ikke er tilknyttet en bankkonto. Brukeren kan, ifølge hjemmesiden easipaycard.no, sette inn "*1000 Euro opp til 15 000 Euro eller et ubegrenset beløp*". Kortet utstedes og markedsføres også i Norge som studentkortet. I Norge er IDT Financial Services registrert hos Finanstilsynet som kredittinstitusjoner som har meldt om grenseoverskridende virksomhet i Norge på grunnlag av annet bankdirektiv.

31

Paygoo
Paygoo kom på det norske markedet i 2016, og tilbyr både ladbare og ikke-ladbare kort. Kortene selges hos Narvesen og 7-Eleven. Kortene kan brukes til kjøp av varer og tjenester på nett og hos forhandlere som aksepterer MasterCard. Paygoo prepaid MasterCard Gift kan fylles hos forhandler med mellom 100 og 2 000 kroner, for Paygoo Prepaid MasterCard reload varierer beløpsgrensen etter grad av identifikasjon. Wirecard card solutions Limited er autorisert for utstedelse av e-penger i England, i Norge er Paygoo registrert som et grensekryssende e-pengeforetak.

32

[30] www.spendon.no Om oss
[31] www.easipaycard.no og www.studentkortet.no om studentkortet Mastercard
[32] www.paygoo.no om oss

Closed loop og restricted loop

Restricted loop kort kan brukes i et utvalg av butikker som velger å knytte seg til en slik betalingsløsning.[33] Det kan være begrensninger som geografi, type firma, type betalingsterminal og så videre. Eksempel på kort som selges i Norge er Universal Presentkort. Slike kort er ikke per i dag ikke regulert som e-penger.[34]

Closed Loop kort har et begrenset bruksområde, eksempelvis et gavekort for en forhandler/kjede. Gavekortene kan ikke brukes overalt, men bare i en butikkjede og kan ikke brukes til uttak i minibank.

Closed loop og restricted loop har begrensede bruksområder og er dermed mindre egnet til å skjule spor etter kriminalitet.

Personlig/ikke personlig

Forhåndsbetalte kort kan være både personlige og upersonlige. Dersom kortet er upersonlig er det som regel ikke nødvendig å oppgi personopplysninger ved kjøp og brukeren forblir anonym. Dersom kortet er personlig registreres eiers personopplysninger.

Ladbart/ikke ladbart

De forhåndsbetalte kortene er ladbare eller ikke-ladbare. På kortene som ikke er ladbare er det bare summen som blir lastet inn ved kjøp som kan benyttes på kortet. Er kortet ladbart kan det gjøres innskudd innen gitte grenser.

Swiss Bankers
Swiss Bankers Prepaid Services AG fra Sveits tilbyr blant annet produktene Travel Cash og Mastercard prepaid. Selskapet er eid av banker, blant annet Credit Suisse AG. Kjerneproduktet til Swiss Bankers er kortet Travel Cash. For å få travel cash må navn, adresse, nasjonalitet og fødselsdato registreres hos Swiss bankers AG. Kortet er tilknyttet Mastercard og kan benyttes der det tilbys betaling med det. Det selges med valutaene Euro, amerikanske dollar eller sveitsiske franc. Kortet er ladbart og maksimalt innestående beløp er 10 000 Euro, USD eller CHF. Maksimal innlasting løpet av et år er 100 000 Euro, USD eller CHF. Det er en begrensning på fem slike kort pr person. Mastercard prepaid er også ladbart og har samme begrensninger på maksimalt innestående beløp. Årlige begrensninger kan imidlertid variere fra person til person. Selskapet utsteder kort på vegne av Credit Suisse. Selskapet har banklisens i Sveits og har et datterselskap i Lichtenstein som har lisens som et e-pengeforetak. Kortene kan bestilles fra sveitsiske banker og fra banker utenfor Sveits.

[35]

[33] www.prepaidcardservises.co.uk Glossary of therms
[34] I det andre betalingstjenestedirektivet (PSD2) åpnes det for at det reguleres som e-penger dersom kortet utvider/utvikler seg og blir mer generell.
[35] www.swissbankers.ch Frequently asked questions, www.swissbankers.ch General terms and conditions for the use of Swiss bankers travel card og www.swissbankers.ch General terms and conditions for the use of Swiss bankers MasterCard prepaid.

Internettbaserte betalingstjenester

Struktur/ mekanismer

Internettbaserte betalingstjenester tilbyr mekanismer for å utføre betalinger over internett mellom kjøpere og selgere, og for personlige overføringer.[36] Det tilbys overføringer og betalinger direkte fra konto til konto, kort-initierte betalinger, betalinger internt i forhåndsbetalte e-wallet løsninger, e-pengeløsninger og rene betalingsformidlere. Internettbaserte betalingstjenester kan også kombineres med for eksempel forhåndsbetalte kort.

Med utgangspunkt i FATFs rapporter er det delt opp i fem kategorier:

- Betalingsformidlere
- Tredjepartstilbydere
- E-wallet
- Faktura
- E-Voucher

Betalingsformidler

Felles for betalingsformidlere er at de formidler betalinger både innenlands og på tvers av landegrensene. Det finnes flere forskjellige typer. Betalingsformidlere kan ha avtaler med internasjonal og lokal betalingsinfrastruktur for overføring av penger. Overføringene blir både billigere og raskere. Tradisjonell bankoverføring derimot, går gjennom flere banker før målet nås med lang overføringstid og høye kostnader. To eksempler på slike betalingsformidlere er Earthport (se faktaboks) og Worldpay.

Earthport
Earthport har sitt hovedkontor i Storbritannia og tjenestene deres tilbys i over 60 land. Deres spesialitet er betalinger på tvers av landegrenser på vegne av banker, virksomheter, betalingsformidlere og gateways. I Storbritannia er Earthport registrert som et betalingsforetak mens det Norge er registrert som grensekryssende betalingsforetak. Earthport har kuttet antall ledd i forhold til vanlige banktransaksjonen slik at transaksjoner kan gå "real time". Gjennom et stort nettverk av samarbeidende banker og blant annet blockchainteknologi får de utført betalinger raskere enn direkte gjennom bank. Det fremkommer ikke beløpsbegrensninger på bruk.

37

[36] FATF Guidance for a risk based approach Prepaid cards, Mobile payments and internet-based payment services, 2013 (Side 9-11)
[37] www.earthport.com About og www.coindesk.com The unsexy way earthport is using shared ledger for blockchain Efficiencies. Gateway er en applikasjon som godkjenner kort betalinger på nett.www.hostmerchantservices.com How payment gateways work.

Tredjepartstilbyder

Det finnes i dag to forskjellige tredjepartstilbydere; betalingsinitieringstjeneste og kontoopplysningstjenester. Det er kun førstnevnte som tilbys i Norge i dag. En betalingsinitieringstjeneste iverksetter en betaling fra en konto hos en annen betalingstjenestetilbyder på vegne av brukeren, mens kontoopplysningstjenester får tilgang til kontoopplysninger for å kunne gi kunden oversikt over alle sine konti.[38] Eksempler på betalingsinitieringstjenester er Sofort, iDEAL og Trustly (se faktaboks). Kun Trustly tilbyr sine tjenester på nett i Norge per i dag.[39] For brukeren kan det være en sikkerhetsrisiko at tredjepartstilbyderne gis sensitiv informasjon som gir tilgang til bankkontoen.[40]

Trustly
Trustly er en betalingsinstitusjon med hovedkontor i Sverige som tilbyr betalingstjenester både i Norge og innen EU/EØS. Selskapet er registrert hos Finanstilsynet som et grensekryssende betalingsforetak. Trustly tilbyr betaling direkte fra bankkontoen. Tjenesten gis tilgang direkte til konti og når kunden betaler velges det hvilken konto det skal trekkes fra. Det er ikke oppgitt at det er beløpsbegrensninger, men det vil imidlertid kunne være grenser knyttet til den enkelte konto.

[41]

E-wallet

En e-wallet er en løsning der penger blir lastet inn på en konto holdt av tjenestetilbyderen for senere å kunne gjennomføre kjøp av varer og tjenester eller overføre til andre uten bruk av betalingskort.[42] Kontoen kan løpende fylles opp med tilknyttede debetkort eller konto, alternativt ved bruk av forhåndsbetalte kort og vouchers. Innestående på slike konti er i lovens forstand e-penger.[43] Et eksempel på en tilbyder av e-wallet er Paypal (se faktaboks) og Skrill. For overføring trengs bare e-postadresse og kunden trenger ikke å taste inn kortopplysninger ved hver handel.

[38] www.regjeringen.no Innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. Utkast til høringsnotat (Side 6)
[39] www.trustly.com Forsiden
[40] www.banking.com PSD2 and its implications for fraud
[41] www.trustly.com
[42] Det danske Betalingsrådet Rapport om nye betalingsløsninger 2013, (side 41 og 42)
[43] Lov 10. april 2015 nr 17 Finansforetakslovens § 2-4: Elektroniske penger (E-penger) er elektronisk lagret pengeverdi representert ved en fordring på utstederen, som er utstedt etter mottak av midler for å utføre betalingstransaksjoner, og som er anerkjent som betalingsmiddel av andre enn utstederen."

PayPal
PayPal er et av verdens største internettbaserte betalingsselskaper med hovedkontor i USA og europakontor i Luxembourg. Selskapet tilbyr tjenester for å handle varer og tjenester på nett og overføring av penger mellom personer på tvers av landegrenser. For å overføre til andre er det kun behov for en e-postadresse. For mottak av penger må brukeren opprette en PayPal-konto. For å overføre må man enten ha overført penger til PayPals e-wallet eller ha et kort tilknyttet e-walleten slik at PayPal kan trekke direkte fra kortet. Store butikker som for eksempel Lefdal og Elkjøp tilbyr betaling med PayPal. I Norge er selskapet registrert som grensekryssende kredittforetak hos Finanstilsynet. PayPal kan etter skjønn innføre begrensninger på hvor stort beløp som kan overføres. Ved å tilknytte et bekreftet betalingskort kan grensen heves.

PayPalkunder hadde innestående totalt 13,02 milliarder amerikanske dollar første kvartal 2016. I USAs største bank, Bank of America, hadde kundene innestående 427,19 milliarder amerikanske dollar på samme tidspunkt. PayPal opplyser på sine hjemmesider at de i 2015 behandlet transaksjoner verdt 282 milliarder amerikanske dollar i hele verden.

[44]

Cash voucher/e-voucher

Cash voucher har mange likheter med forhåndsbetalte kort, og er et forhåndsbetalt produkt (e-penger) som kan brukes for å betale forhandlere eller overføre til andre personer.[45] Disse kan kjøpes anonymt for kontanter i butikk eller online. Cash vouchers består av koder som også kan benyttes til å fylle opp andre nyere betalingstjenester eksempelvis e-wallets. Ved bruk autoriserer eier av e-voucheren at utstederen betaler forhandleren og reduserer innestående e-penger.[46] Eksempler på vouchers er, Swiftvoucher (se faktaboks), EMP Corp og Paysafecard (se faktaboks).

Swiftvoucher
Swiftvoucher er forhandler av iCheque vouchers. iCheque vouchers er koder som kan brukes for handel på nett og kan også brukes til å sette penger inn hos spillselskaper. Fordeler som nevnes av Swiftvoucher.com er at man kun oppgir koden overfor nettsteder og ikke kortnummer og bankkontonummer. Swiftvoucher er registrert i Gibraltar, og iCheque registrert i Malta. iCheque har konsesjon som e-pengeforetak i Storbritannia, mens Swiftvoucher/Easterbrook Limited er autorisert distributør av iCheque vouchers. I Norge er iCheque Network LTD registrert som et e-pengeforetak. Man kan kjøpe vouchers fra Swiftvoucher.com, med en begrensning på 50 000 kroner per kjøp.

[47]

[44] www.paypal.com Om oss, FATF ML using new payment methods, 2010 (side 8), www.elkjop.no betalingsalternativer og marketwatch.com
[45] FATF ML using new payment methods, 2010 (side 25)
[46] www.emexpay.com Emexpay evouchers terms and conditions
[47] www.Swiftvoucher.com faqs, www.icheque.com how it works

Paysafecard
Paysafecard er en voucher man får kjøpt i butikker (Narvesen, Kiwi og 7 eleven) for å betale på nettet. Paysafecard er registrert i Østerrike og Prepaid Services Company Limited i Storbritannia. Paysafecard er et datterselskap av Paysafe Group plc Subsidiary. I Norge er Prepaid Services og Paysafecard.com begge registrert som grensekryssende e-pengeforetak. Koden som står på voucheren tastes inn ved betaling i nettbutikker. Kunden trenger ikke å registrere seg. Man kan velge mellom verdiene 100, 250, 500 eller 1 000 kroner.

48

Faktura

Utstedelse av faktura er ikke nytt. Det er imidlertid et nyere konsept at en tredjepart står for fakturering av kunden. Et eksempel på en slik tjeneste er Klarna.[49]

Mobile betalingstjenester

Mobile betalingstjenester er bruk av mobiltelefon eller annet trådløst kommunikasjonsutstyr til å kjøpe varer og tjenester.[50] [51] Betaling kan utføres gjennom mobilapplikasjoner, internett eller SMS. I Norge er smarttelefoner med tilkobling til internett svært utbredt. 89 prosent av Norges befolkning hadde per fjerde kvartal 2016 en smarttelefon. I aldersgruppen 12-49 år har 99 prosent smarttelefon.[52]

Det er vanligst å bruke mobiltelefon for å godkjenne betaling fra betalingskort eller konto. Dette er en utvidelse av de tradisjonelle metodene for betaling. Nyere måter å betale på er at teleoperatøren eller et teknologiselskap opererer som mellomledd for betaling på to måter, forhåndsbetalt eller på etterskudd:[53]

Mobile betalingstjenester kan i utgangspunktet deles opp i fire: Mobil wallet, telefaktura, betalingsformidler og tredjepartstilbyder.

Mobil wallet, telefaktura og mobile tredjepartstilbydere

Eksempel på mobil wallet er Paypal og Skrill, som tilbys i Norge og er internettbaserte løsninger som også tilbys på mobil.[54] Det finnes også løsninger der teleoperatøren er

[48] www.paysafecard.com
[49] www.klarna.no
[50] FATF Report on New payment methods, 2006 (Side 6-7)
[51] "Annet trådløst kommunikasjonsutstyr": Eksempelvis tablet
[52] Statistikk fra Kantar TNS kvartalsvise interbuss undersøkelse, www.medier24.no Nå har 99 prosent av alle mellom 12 og 49 år en smarttelefon
[53] FATF Money laundering using new payment methods, 2010 (Side 18-19)
[54] Kommunal og moderniseringsdepartementet, Markedet for innovative, digitale betalingstjenester, omtalt i denne rapporten som "internettkonto" (Side 21-22)

den som stiller med konto, eksempelvis mPesa. En mobil wallet kan brukes til å handle i nettbutikker, overføring til andre, og betale i butikk tilknyttet trådløs teknologi (NFC).[55]

Telefaktura fungerer på samme måte som fakturatjenester beskrevet under internettbaserte betalingstjenester.[56] Betaling skjer enten gjennom mobilfaktura eller faktura direkte fra tilbyderen av løsningen. Eksempel på en slik mobil tjeneste er Strex.

Strex
Strex er et selskap som ble registrert i 2003 og som eies av Telenor, Telia og ice.net. Selskapet tilbyr en mobil løsning for betaling gjennom mobilabonnementet eller faktura direkte fra Strex. Løsningen kan blant annet benyttes hos Easypark og Ruter. Strex AS er registrert hos Finanstilsynet som et e-pengeforetak. Ved avtale om faktura direkte fra Strex sendes faktura dersom beløpet overstiger kr 3 000. Maksimal kredittgrense hos Strex er 5 000 kroner.

[57]

Mobile tredjepartstilbydere er tilbydere som initierer eller starter en betaling på vegne av brukeren, enten ved bruk kort eller direkte fra bankkonto. Dette benyttes i butikk med trådløs teknologi eller handel på nett. Internasjonale aktører her er Apple pay (se faktaboks) og Android Pay, men løsningene er ikke tilgjengelig i Norge per i dag.

Apple Pay
Apple Pay er en mobil applikasjon som ble lansert av amerikanske Apple i 2014. Apple produktene benyttes på plattformene iphone, ipad, Apple Watch og Macbook pro med touch id. Ved å legge inn kortdetaljer kan betalinger skje på nett eller trådløst i butikk. For å gjøre betalingen sikker sender ikke Apple Pay kort detaljene, men sørger for at en betaling initieres ved at et kryptert "konto nummer" sendes. Apple Pay er en av flere større internasjonale aktører som enda ikke har lansert sine tjenester i Norge.

[58]

Mange mobile betalingstjenester fungerer på samme måte som beskrevet under internettbaserte betalingstjenester. Flere av de nevnte tilbys ikke i Norge og noen er internettbaserte som også tilbys på mobil. På bakgrunn av dette går vi i dokumentet ikke nærmere inn på mobil wallet, telefaktura og mobile tredjepartstilbydere.

[55] NFC (Near field communication) - En teknologi som muliggjør betaling trådløst. Telefonen må da være i nærheten av en sender ved kassen som gjør at telefon og kasse kommuniserer. www.techradar.com What is nfc
[56] www.fortumo.com products
[57] www.strex.no
[58] Apple.com/apple-pay, www.24solutions.com PSD2 whitepaper (Side 4)

Betalingsformidler

Løsningen innebærer at bruker har registrert og lagret bank- eller kredittkortopplysninger i en applikasjon på telefonen. På denne måten kan vedkommende betale i butikk ved bruk av trådløs teknologi, overføre til andre eller betale på nett. Eksempel på slike løsninger i Norge er MobilePay og Vipps (se faktabokser). Bank- eller kredittkortene til tjenestene som tilbys i Norge må være tilknyttet konto i norsk bank. Det er på det nåværende tidspunktet bare betalingsformidlere som tilbyr sine tjenester på mobil i Norge.

MobilePay
MobilePay ble etablert i 2013 av Danske bank og er en mobil betalingsløsning som tilbys av danske bank. Man kan betale i butikk med trådløs teknologi, overføre til andre eller be om betalinger fra andre. Når kunden betaler går pengene til MobilePay før de utbetales til mottaker. Kun konto, debet- eller kredittkort utstedt fra et norskt foretak kan knyttes opp mot tjenesten. I tillegg må man oppgi et norsk telefonnummer og fødselsnummer. Maksimalt 22 000 kroner kan sendes per kalenderår. Registrering med bankID gir høyere beløpsgrenser.

[59]

VIPPS
Vipps ble lansert i 2015 og er mobil betalingstjeneste for overføring mellom personer og for betaling hos lag og foreninger, i butikker og på nett som har et samarbeid med Vipps. Kun norsk mobiltelefonnummer og bankkonto, kredittkort eller debetkort utstedt av norske banker kan benyttes. Man kan sende penger til alle med norsk mobiltelefonnummer. Betaling går via DNB før det videresendes til mottaker. 22 000 kroner kan sendes per år, benyttes bankID er grensen 250 000 kroner per år. Vipps eies av DnB, Sparebank1, Eika, Sparebanken Møre og 15 selvstendige sparebanker som alle har konsesjon som bank hos Finanstilsynet. DnB er største eier med 51 prosent av aksjene.

[60]

[59] www.mobilepay.no, vilkår og www.danskebank.no Nettbank og mobil
[60] www.vipps.no vilkår

Virtuell valuta

Virtuell valuta er mye omtalt i media, særlig Bitcoin. Både i forbindelse med økt verdi, investeringspotensiale, bankers omfavnelse av Bitcoin og i forbindelse med bruk i kriminalitet.[61]

European Central Bank (ECB) definerer virtuell valuta som: "En digital representert verdi som ikke er utstedt av en sentralbank, kredittinstitusjon eller e-penge institusjon, men som i noen tilfeller kan bli brukt som et alternativ til penger." [62]

European Banking Authority (EBA) trekker i sin definisjon også inn "ikke nødvendigvis knyttet til en konvensjonell valuta, men som er akseptert av fysiske eller juridiske personer som et betalingsmiddel og kan bli overført, lagret eller handlet elektronisk".[63]

Virtuell valuta tilbyr mekanismer for å overføre verdier mellom personer på nettet, og for kjøp og salg av varer på steder der virtuell valuta aksepteres som betalingsmåte. De mest utbredte virtuelle valutaene er krypterte og betegnes kryptovaluta. Kryptovalutaene har store svingninger i kursene og blir av den grunn mye brukt til spekulasjon.

Virtuelle valutaer er ikke utstedt eller garantert av noen myndigheter og fungerer ved at brukerne har felles tillit til at valutaen har en verdi. Videre har virtuell valuta i motsetning til e-penger ikke en direkte kobling mot reell valuta.[64]

Kategorier

Virtuell valuta kan deles inn i tre kategorier: lukkede, enveisflyt og toveisflyt. Oppdelingen er basert på European Central Banks rapport Virtual Currency Schemes.[65]

Toveisflyt

Virtuelle valutaer med toveisflyt kan veksles med reell valuta. Denne typen valuta har likheter med reell valuta da den kan benyttes til å kjøpe varer og tjenester, virtuelle og fysiske. Eksempler på virtuelle valutaer med toveisflyt er Bitcoin og Ethereum.

Enveis flyt og lukkede virtuelle valutaer

Virtuelle valutaer med enveisflyt kan kjøpes med reell valuta, men kan ikke veksles tilbake til reell valuta. Denne valutatypen kan brukes til å kjøpe både virtuelle og fysiske varer og tjenester. Eksempler på dette er Amazon Coins og Nintendo Points.

Lukkede virtuelle valutaer har ingen kobling med reell valuta. De virtuelle pengene opparbeides/erverves virtuelt og brukes virtuelt. Dette er ikke uvanlig i spillverdenen.

Enveis flyt og lukkede virtuelle valutaer har begrenset eller ingen kobling til en reell valuta. Det kan imidlertid finnes et svart marked for kjøp og salg av valutaene.[66]

---

[61] www.omni.se Nordea oroas över bitcoin-kopplad kriminalitet
[62] European central bank (ECB) Virtual currency schemes 2015 (Side 25)
[63] European banking authority (EBA) Opinion on "Virtual currencies" juli 2014 (side 5)
[64] Med reell valuta menes penger som er utstedt av en sentralbank ("Fiat penger") www.oest.no Penger, gull og fiat
[65] Fra Oktober 2012 (side 13-15)
[66] FATF Virtual currencies Key definitions and potential aml AML risks, 2014 (Side 5)

Struktur

Sentralisert/desentralisert

Ved sentralisert virtuell valuta står en administrator (tredjepart) bak og kontrollerer systemet.[67] Administratoren utsteder, lager regler for bruk, opprettholder en sentral transaksjons-reskontro og har autorisasjon til å ta valutaen ut av sirkulasjon. Vekslingsgebyret for å konvertere den virtuelle valutaen kan enten være flytende eller fast, satt av administratoren. Eksempler er Linden Dollars og Wow gold.

Desentralisert virtuelle valutaer har ingen sentral administrerende myndighet og ingen sentral overvåkingsmyndighet. Valutaene er distribuerte, har åpen kildekode, er matematikkbaserte og organiserte som såkalte peer-to-peernettverk. Eksempler på desentraliserte valutaer er Bitcoin, Ethereum og Ripple.[68] [69]

Kryptovaluta

Mange av de virtuelle valutaene er såkalte kryptovalutaer.[70] De har toveisflyt, er matematikkbasert, desentraliserte og er beskyttet med kryptografi.[71] I sin enkleste form krypteres det for å gjøre data uleselig eller utilgjengelig, og motsatt for å gjøre data leselig eller tilgjengelig. Kryptografi i kryptovalutaer baserer seg på offentlige og private nøkler for å overføre fra person til person. Et eksempel på en kryptovaluta er Bitcoin.

En privat nøkkel er "billetten" som lar brukeren benytte den virtuelle valutaen i en transaksjon, eksempelvis Bitcoins.[72] En privat nøkkel ser typisk slik ut:

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydyXYB9KF

Denne typen private nøkkel henger sammen med en offentlig nøkkel og er på 51 tegn og starter alltid med 5 eller 9. Dersom nøkkelen blir borte er det ikke mulig å få tilgang til pengene og pengene er tapt, dette da koden er eneste inngang til dem. I en sak fra Wales, beskrevet i The Guardian, hevdet en person å ha kastet en harddisk med 7 500 bitcoins med en total verdi på fire millioner Euro.[73]

---

[67] FATF Virtual currencies Key definitions and potential aml AML risks, 2014 (Side 5)
[68] Peer to peer nettverk er to eller flere pcer koblet sammen og deler datakraft uten å gå gjennom en sentral server. www.computerworld.com peer-to-peer network
[69] www.computer.org – A definition of Peer-to-peer networking..: I et peer to peer nettverk er ressursene (filer, behandlingskraft, overføringskapasitet og kortidslagring) delt på flere lokalt administrerte klientprosesser. Dette er i motsetning til et serverbasert nettverk der ressursene ligger på sentrale servere som er sentralt administrert:
[70] FATF Virtual currencies-Key definitions and potential AML/CFT risks, 2014 (Side 5)
[71] doc.lagout.org Cryptography for dummies (Side 28)
[72] en.bitcoin.it Private key
[73] www.theguardian.com Hard drive containing Bitcoins worth £4m in Newport

Den offentlige nøkkelen kan sammenlignes med et bankkontonummer og kalles i kryptovalutaen Bitcoin for Bitcoin-adressen.[74] Denne kan deles med andre for å kunne motta den virtuelle valutaen. For å sende den virtuelle valutaen må det benyttes en privat nøkkel som er godkjent av den offentlige nøkkelen. Et eksempel på en offentlig nøkkel eller Bitcoin-adresse er:

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2.

De kan starte på 1 eller 3 og lengden er på mellom 26-36 tall/bokstaver.

Et nettverk av aktører (i Bitcoin kalt minere) opprettholder sikkerheten, integriteten og balansen i en kryptovaluta. Minere får et forhåndsbestemt beløp for jobben. I Bitcoin får de en andel av de nyutvunnede Bitcons, i andre tilfeller får de et beløp for å inkludere deres transaksjoner i den neste "blokken".

De åtte største kryptovalutaene er Bitcoin(se faktaboks), Ethereum (se faktaboks), Ripple, NEM, Ethereum Classic, Litecoin, Dash og Monero.

Ethereum
Ethereum er en toveis flyt, desentralisert, kryptobasert virtuell valuta og bruker blockchainteknologi. Dette er den nest største kryptobaserte virtuelle valutaen målt i markedsandel. Den ble opprinnelig lansert i 2014 av sveitsiske Ethereum Foundation. Ether er navnet på verdienheten. Ethereum kan knyttes opp mot wallets for eksempel i coinbase, mist og Ethereum.

[75]

[74] en.bitcoin.it Address
[75] www.coinmarketcap.com forsiden og www.ethereum.org forsiden

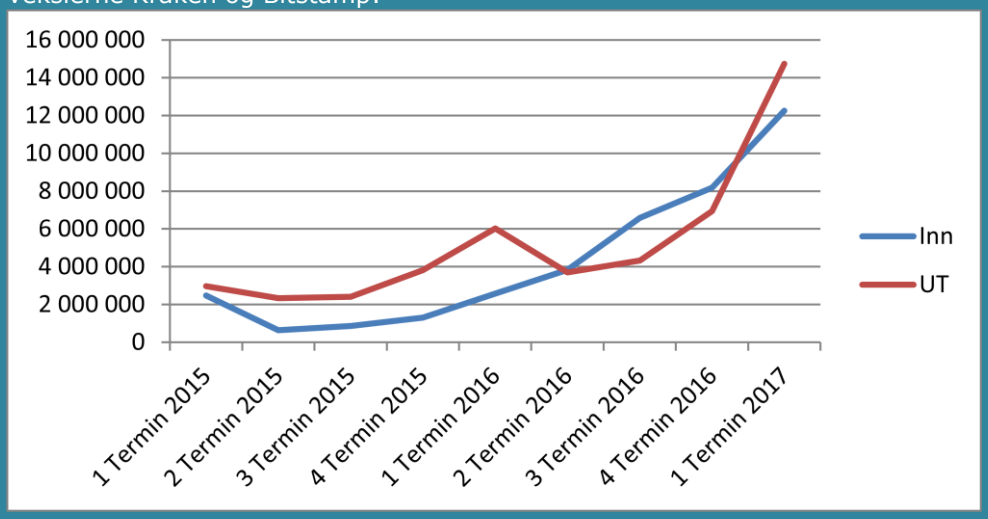
Bitcoin

Bitcoin er en kryptert virtuell valuta med toveisflyt, som er desentralisert, peer to peer. Bitcoin ble utgitt som en åpen kildeprogramvare i 2009.[1] [2] Aliaset Satoshi Nakamoto står bak Bitcoin, men det er ukjent om dette er en person eller om det er en gruppe med programmerere som står bak.[3] Kryptering benyttes for å forhindre forfalskninger eller at Bitcoins blir benyttet mer enn en gang. Det er i dag den klart største virtuelle valutaen målt i markedsverdi. Bitcoin blir utvunnet og godkjent gjennom "mining". Bitcoin kan veksles med andre valutaer og til kjøp av varer og tjenester, det er foreløpig ikke mange forhandlere som aksepterer Bitcoin i Norge.[4]

Satoshi Nakamoto bestemte at det skal være en begrensning på 21 millioner Bitcoins. Det anslås at cirka 75 prosent av alle Bitcoins vil være utvunnet i 2017.[5]

Bitcoin er akseptert som betalingsmiddel i Japan, Kina, Frankrike og Tyskland. Det finnes en minibank for uttak av Bitcoin og andre kryptovalutaer i Oslo. Man finner også en i Stockholm, elleve i Helsingfors (15 i hele Finland) og tre i København.[6] Eksempler på selskap som aksepterer Bitcoin er Windows, Dell, AirBaltic, Air Lituania.

Det har vært kraftig økning i antall transaksjoner på verdensbasis med Bitcoin fra den spede start i 2009: Fra 2014-2016 har det vært en økning på hele 57 millioner transaksjoner, fra 25 millioner til 82 millioner transaksjoner, anslag for 2017 er 102 millioner transaksjoner.[7] Det har totalt vært en omsetningsøkning fra 2012 til 2016 på 878 prosent.
Tabellen nedenfor er tall hentet fra valutaregisteret og viser veksling til og fra Norge fra vekslerne Kraken og Bitstamp:



Økningen i transaksjoner inn til Norge fra nevnte vekslerne i utlandet fra 01.01.16 til 31.03.17 er fra 2 millioner kroner til overkant av 12 millioner kroner.

76

76
1. FATF Virtual currencies – Key definitions and potential AML/CFT risks, 2014 (Side 5)
2. bitcoin.org forsiden - Designet er offentlig, ingen eier eller kontrollerer bitcoin
3. www.allenovery.com Legal & regulatory risk note (Side 50)
4. norgesbitcoinforening.no Hvor kan jeg bruke bitcoins
5. www.metzdowd.com Bitcoin P2P e-cash paper
6. Coindesk.com bitcoin atm map
7. Data hentet ut 22.05.17 fra data.bitcoinity.org. Kilden deres er alle vekslernes API. Data.bitcoinity.org drives av Kacper Ciesla. Tall fra 1. kvartal 2017 er benyttet for å gjøre anslag for 2017

Viktige funksjoner

Distribuert hovedbok/Blockchain[77]

Det som muliggjør transaksjoner uten en tredjepart er hovedboken som er distribuert til alle deltakerne (noder) i et nettverk.[78] Dette skjer uten hensyn til landegrenser, eller en sentral lagringsenhet eller administrasjon. I Bitcoin heter denne Blockchain.

"En blockchain er et nettverk av datamaskiner, der alle medlemmer av nettverket sitter på en kopi av en felles offentlig "reskontro" (transaksjonsoversikt). Alle har innsyn i reskontroen, men ingen kan endre i den. Reskontroen er bygget som en lenket liste eller kjede av blokker, der hver blokk inneholder en rekke transaksjoner som er blitt utført i et gitt tidsrom."[79]

Hver gang en transaksjon blir godkjent av noder legges transaksjonen til i Blockchain.[80] [81] Dette skjer cirka seks ganger per time, det samles opp flere transaksjoner og legges samlet inn og publiseres til alle nodene. Ved betaling fungerer det som ved en kontanttransaksjon. Dersom du har mottatt tre Bitcoin tidligere i en transaksjon og skal bruke dem til å betale to Bitcoin, må du først betale tre og så få tilbake vekslepengene, én Bitcoin.[82] Hver blokk i en blockchain har informasjon om transaksjonen, dato, og kryptert informasjon om den foregående blokken pluss nonce.[83]

Wallet – oppbevaring av Virtuelle valutaer

Virtuell valuta wallet er et medium (program eller annen mekanisme) for å oppbevare og overføre virtuelle valutaer.[84] En wallet holder brukerens private nøkkel. Det finnes to typer wallet, "kald" og "varm" wallet. Varm wallet ligger på nett (Web Wallet), mens kald wallet er et lagringsmedium som ligger utenfor nettet (harddisk, minnepinne, papir og så videre).

På siden Bitcoin.org fremkommer mange wallets som anbefales for Bitcoin. Eksempler er Xapo, Coinbase, Blockchain, Trezor, Exodus og MyCelium.[85] Høy grad av sikkerhet tilbys med tilgang på mobil og i tillegg debetkort tilknyttet Visa knyttet direkte opp mot Bitcoin.

Viktige roller i omsetning og bruk av virtuelle valutaer

Veksler –En person eller enhet som veksler virtuell valuta til reell valuta eller andre former for virtuell valuta, inkludert veksling til og fra edelt metall for en avgift.[86] Eksempler på vekslere er OKCoin, Kraken og Bitstamp.[87] Vekslere kan godta

---

[77] "Distributed ledger"
[78] Sprint.no Hva er egentlig blockchain
[79] www.evry.com Banktjenester via blockchain
[80] Noder er deltakerne i et desentralisert peer to peer nettverk. bthusby.silvrback.com Hvordan fungerer Blockchain?
[81] bitcoin.org Bitcoin: A Peer-to-peer electronic cash system
[82] www.TU.no - Hvordan virker Blockchain www.tu.no blockchain er teknologien som gjor det mulig a se om noen har hacket seg inn i eller endret data
[83] bitcoin.org Bitcoin: A Peer-to-peer electronic cash system. Nonce er et tall som bare kan brukes en gang og er helt vilkårlig
[84] FATF Virtual currencies – Key definitions and potential AML/CFT risks, 2014 (Side 7–8)
[85] 99bitcoins.com har rangert 5 sistnevnte som 2017s beste bitcoin wallet i 2017
[86] FATF Virtual currencies – Key definitions and potential AML/CFT risks, 2014 (Side 7)
[87] data.bitcoinity.org Bitcoin trading volume

bankoverføringer og forhåndsbetalte kort. Ved å benytte lokal veksler er begrensningene hvilken type betalinger vedkommende godtar. I tillegg til de betalingsmåtene allerede nevnt kan dette involvere kontanter og internettbaserte betalingstjenester.

Miner – En miner er et individ eller enhet som deltar i et desentralisert virtuelt valutanettverk ved å kjøre spesiell programvare for å løse komplekse algoritmer i et distribuert system brukt til å godkjenne transaksjoner i det virtuelle valuta systemet.[88] Minere kan også være brukere.

Kjøpere/selgere – Brukere av virtuelle valutaer er personer som oppbevarer og bruker valutaene til kjøp og salg av virkelig eller virtuelle varer eller tjenester eller som en personlig investering.[89]

Skattemessige konsekvenser

Ved bruk av virtuelle valutaer har privatpersoner skatteplikt på realisasjon. I tillegg regnes virtuelle valutaer som formuesobjekt og privatpersoner har dermed skattepliktig formue uansett hvor i verden eiendelene befinner seg.[90]

Trender

Det er store endringer innen betalinger. Særlig gjelder dette endrede kundeforventninger og ny innovativ teknologi. Noen av trendene beskrives nærmere:

Økt konkurranse på markedet

Det andre betalingstjenestedirektivet (PSD2) skal innføres 13.1.2018. Bankene må da legge til rette for å gi betalingstjenestetilbydere tilgang til bankens betalings- og kontosystemer.[91] Det blir i denne forbindelsen tilrettelagt for to nye typer betalingstjenester, betalingsinitieringstjenester og kontoopplysningstjenester. Finansielle teknologiselskaper eller gründerselskaper kan benytte seg av bankdata for å gi kundene innovative og nyttige fremstillinger av kundedata.[92]

Resultatet er en ytterligere oppstykking av verdikjeden for betalinger. Målet er at det skal føre til mer konkurranse og flere fordeler for kundene. For bankene er konsekvensen at nye aktører overtar kontakt med kundeflaten. For etatene kan konsekvensen bli at nye, utenlandske, aktører besitter informasjonen bankene tidligere hadde oversikt over.

Nordea lanserte i mars 2017 en mulighet for startups eller gründerselskaper å benytte bankens betalings- og kontosystemer og ut fra dette utvikle nye tjenester tilpasset bankens data. I løpet av 24 timer hadde 130 startups registrert sin interesse.[93]

---

[88] FATF Virtual currencies – Key definitions and potential AML/CFT risks, 2014 (Side 7)
[89] FATF Virtual currencies – Key definitions and potential AML/CFT risks, 2014 (Side 7)
[90] www.skatteetaten.no Skattemessige konsekvenser ved bruk av bitcoins og andre virtuelle valutaer for privatpersoner
[91] Se nærmere om PSD2 i vedlegg 2.
[92] Fintech - Finansielle teknologiselskaper se vedlegg 1 for definisjon
[93] www.shifter.no Nordea inviterer startups open banking 130 registrerte pa 24 timer

I Norge har de etablerte mobile betalingstjenestene Vipps og MobilePay inngått samarbeid med flere norske banker. Dette for å møte konkurranse fra globale aktører som kan komme med innføringen av PSD2. Både Facebook og Amazon har meldt om grensekryssende virksomhet som betalingsforetak til Norge. Det forventes også at Apple og Google vil gjøre sin inntreden i Norge.[94]

Virtuelle valutaer

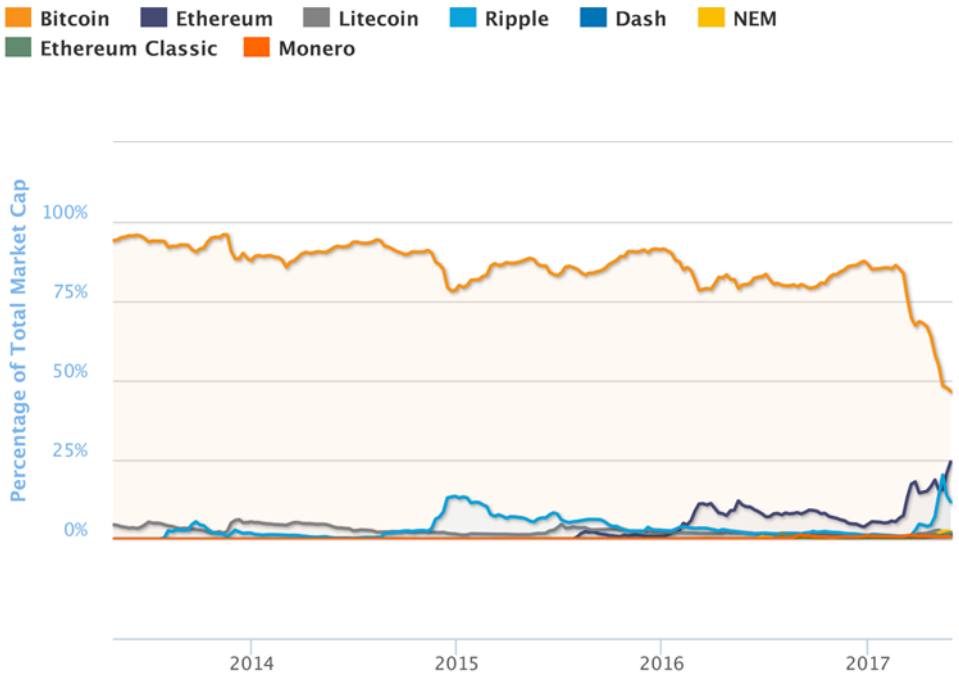
Stadig flere land godkjenner bruk av virtuelle valutaer. Japan har nylig godkjent bruk av virtuelle valutaer og det er ventet at så mange som 260 000 brukersteder vil akseptere virtuelle valutaer allerede i løpet av sommeren 2017.[95]

I Norge har Skandiabanken åpnet muligheten for å se saldo av Bitcoins i nettbanken.[96] Brukerne vil kunne logge seg inn på handleplassen Coinbase gjennom nettbanken. Det kan ikke foretas kjøp og salg av Bitcoin her. Nets har på sin side inngått samarbeid med Chainalaysis. Chainalysis kan validere Bitcoin transaksjoner.

Den 2.3.2017 passerte verdien av en Bitcoin for første gang verdien av en unse gull. På det tidspunktet var en Bitcoin verdt 1 275 dollar mens en unse gull kostet 1 232 dollar.[97] Den 25.5.17 var verdien av én Bitcoin oppe i 2 357 dollar.[98] Kursen på Bitcoin har hatt store svingninger i løpet av det siste året. Årsaken til dette forklares blant annet med høy etterspørsel i Kina. Der benyttes Bitcoin til å overføre penger til utlandet, men også til spekulasjon.[99]

[94] www.finanstilsynet.no Risiko og sårbarhetsanalyse 2016 (Side 12)
[95] www.dn.no Venter 50 dobling i brukersteder for digitale valutaer
[96] www.e24.no Nå får du bitcoin i nettbanken
[97] www.coindesk.com Price
[98] www.coindesk.com Price
[99] www.e24.no Nå er bitcoin dyrere enn gull

Bitcoin er per 1. juni den største av de virtuelle valutaene og har en markedsverdi som er 45 prosent av den totale markedsverdien. Imidlertid øker mange andre virtuelle valutaer mer og Bitcoin har tapt markedsandel.[100]



Figur: Klippet ut fra nettsiden coinmarketcap.com og viser markedsverdien til de 8 største kryptovalutaene.

Ethereum er den nest største virtuelle valutaen, med en markedsverdi på 25 prosent. Totalt har 107 kryptovalutaer en markedsverdi på over 10 millioner dollar.[101]

Nettsedler

Norges bank forholder seg også til utviklingen som skjer på området og ønsker å følge Norges befolkning inn i den digitale fremtiden.[102] Norges Bank skal utrede en innføring av "nettsedler". Sedlene vil fungere som dagens kontanter der staten og sentralbanken står bak. De elektroniske sentralbankpengene kan gi mulighet for umiddelbart oppgjør og anonyme brukere. Dette trenger ikke nødvendigvis å bety at kontanter skal elimineres helt da dette er en god reserveløsning, sikrer konkurranse og har andre egenskaper. Sverige vurderer også en type elektronisk penge.

[100] www.coinmarketcap.com Percentage of total market capitalization (Dominance)
[101] www.coinmarketcap.com Cryptocurrency market capitalizations
[102] Artikkel fra Aftenposten Innsikt "Også Norge kan få en helt ny type penger"

Kapittel 2: Nyere betalingstjenester og sporbarhet

Hvilke spor legger nyere betalingstjenester

Når nyere betalingstjenester benyttes, legger transaksjonen igjen spor som kontrolletatene kan undersøke. Det legges elektroniske spor lokalt på datamaskinen, servere og mobiltelefonen som benyttes for å gjennomføre transaksjonen.[103] Videre legger transaksjonen spor hos brukerstedet, hos aktører som tar del i aktivering av/ innskudd på den aktuelle betalingstjenesten, eller bruk av/uttak fra den, samt hos tilbyder av tjenesten.[104] Dersom transaksjonen er grensekryssende vil den som regel være rapportert til valutaregisteret.

Muligheter for å forfølge de ulike sporene, avhenger av

- hjemler for innhenting av opplysninger i egen etat, samt
- hvilke opplysninger som er tilgjengelige, være seg et betalingskortnummer, fødselsnummer eller organisasjonsnummer, eller kunnskap om en mistenkelig transaksjon.[105]

Her følger en gjennomgang av hvor etatene kan finne spor av transaksjoner som har gått gjennom nyere betalingstjenester, samt hvilke utfordringer med sporbarhet bruk av tjenestene representerer for etatene.

Forhåndsbetalte kort

Utsteder av det forhåndsbetalte kortet mottar informasjon fra innløser om alle transaksjoner hvor kortet benyttes.[106] Eksempelvis blir all bruk av SpendOn VISA

[103] Elektroniske spor er spor som noen av de involverte har avsatt elektronisk, jf. Etterforskingsmetoder – en innføring, Bjerknes og Johansen 2010.
[104] Det er en generell utfordring at bruker kan ha benyttet falsk eller stjålet identitet ved registrering hos tilbyder. Falsk identitet er lett tilgjengelig på Darknet. Manglende krav til tilstrekkelig legitimasjon hos enkelte utenlandske tjenestetilbydere bidrar til å forsterke problemet.
[105] Etatenes hjemler er kort beskrevet i Kapittel 4: Politi- og kontrolletatenes erfaringer med nyere betalingstjenester – Nærmere om etatenes erfaringer.

Gavekort rapportert til Sparebank 1 SMN fra innløser. Det vil være mulig å innhente transaksjonshistorikk fra utsteder dersom kortnummeret er kjent. Det vil imidlertid ikke være mulig å knytte dette direkte til eier eller bruker av kortet hvis det er et anonymt kort. Utsteder har ikke informasjon om betalingsmiddelet som er benyttet ved kjøp av kortet.

Transaksjonen vil fremgå av kjøpers kontoutskrift dersom bankkort er benyttet ved kjøp av det forhåndsbetalte kortet.

Brukerstedet kan ha videoopptak av kortbruker, som kan bidra til identifisering. Hovedutfordringene med video fra et brukersted, er kort lagringstid og at foto av kortbruker i seg selv ikke er tilstrekkelig for identifisering.

Bruk av forhåndsbetalte kort som innebærer grensekryssende transaksjoner rapporteres til valutaregisteret på lik linje med andre betalingskort.

Utsteder av kortet er rapporteringspliktig til valutaregisteret når det forhåndsbetalte kortet benyttes i utlandet. *Innløser* er rapporteringspliktig til valutaregisteret når utenlandske kort benyttes i Norge.

Opplysninger som rapporteres til valutaregisteret som kan bidra til å identifisere bruker av kortet fremgår av tabellen under.[107]

	Bruk av norske kort i utlandet		Bruk av utenlandske kort i Norge			
	Enkelttransaksjoner over kr 25 000	Transaksjoner med lavere beløp - sum pr. land pr. mnd	Enkelttransaksjoner over kr 25 000	Transaksjoner med lavere beløp - sum pr. mnd.	Transaksjoner med lavere beløp - sum pr. brukersted	Kontantuttak over kr 5 000
Kortnummer						
Eier av kortet*						
Brukersted						
Aktuelt utland						

*hvis ikke anonymt

De seks første sifrene i kortnummeret er et Issuer Identification Number, også kalt Bank Identification Number (BIN-nummer). Nummeret identifiserer banken eller utstederorganisasjonen. Det kan gjøres søk på enkeltnummer på ulike databaser som er tilgjengelig på nett, eller det kan abonneres på en BIN-database.

Internettbaserte betalingstjenester

E-Wallet

Der bankkort er benyttet til å gjøre overføringer til en e-wallet, vil transaksjonen fremgå av brukers kontoutskrift.[108] Tilsvarende vil det fremgå av kontoutskrifter dersom beholdning på wallet føres inn på bankkonto.

Overføringer til og fra wallets hos utenlandske tjenestetilbydere skal fremgå av valutaregisteret. Utenlandske tilbydere har mulighet til å disponere bankkonti i Norge

[106] Se vedlegg 1 for beskrivelse av utsteder og innløser
[107] Felt merket med rødt indikerer at opplysning ikke rapporteres for den type transaksjon
[108] Om e-wallet – se Kapittel 1: Beskrivelse av nyere betalingstjenester – Internettbaserte betalingstjenester – E-wallet

hvor transaksjonen først blir overført til. Dette medfører at brukeres overføringer til eller fra wallets allikevel ikke fremgår av valutaregisteret.

Noen wallet-tilbydere tilbyr betalingskort knyttet til walleten. Da kan bruker benytte midlene på walleten på alle brukersteder som godtar VISA og Mastercard. Slike transaksjoner vil innløser rapportere til valutaregisteret på lik linje med andre utenlandske kort benyttet i Norge.[109] Det innebærer at enkelttransaksjoner med beløp over 25 000 kroner rapporteres i sin helhet, mens transaksjoner med lavere beløp summeres i månedlig rapport per kort.

Annen bruk av beholdning på wallet, som overføring til annen wallet, betaling for varer eller tjenester og uttak, vil ikke være tilgjengelig for norske myndigheter via valutaregister eller norske tredjeparter. Dette med mindre beholdningen benyttes i Norge og dermed skal rapporteres til valutaregisteret.

Tilgang på kontoinformasjon er en god kilde til dokumentasjon om brukers beholdning og bevegelser. Brukers påloggingsdetaljer, eventuelt utskrift av transaksjonshistorikk, er derfor av stor interesse i saker hvor nyere betalingstjenester er benyttet.

Tjenestetilbyder har oversikt over bevegelsene på wallets. Tjenestetilbyder er forpliktet til å foreta kundekontroll dersom beholdningen er over 250 Euro. Det vil derfor være naturlig å henvende seg til den aktuelle tilbyderen for nærmere informasjon om bruker og transaksjoner, dersom tilgang på transaksjonshistorikk fra bruker ikke er aktuelt.

Tjenestetilbyders morselskap er ofte den som anses å *eie* transaksjonen, og er dermed den som har informasjon om hele transaksjonskjeden. Henvendelse må da rettes til det utenlandske morselskapet i konsernet.

Vouchers

Dersom bankkort er benyttet ved kjøp av voucher, vil transaksjonen fremgå av kjøpers kontoutskrift.[110]

Kjøp av vouchers på nett vil fremkomme av valutaregisteret som korttransaksjoner ut av Norge til tilbyder av tjenesten, for eksempel Swiftvoucher. Identifisering av videre bruk av kodene, vil ikke vises. Kjøp av vouchers i butikk i Norge, vil ikke fremgå av valutaregisteret.

Vouchers har en lav øvre beløpsgrense (1 000 kr) som innebærer at kjøper ikke trenger å identifisere seg. Det er imidlertid sett eksempler på at tilbyderen har kunnskap om betalingsmiddelet benyttet ved kjøp av vouchers, og ut fra kortnummeret kan utlede hvem kjøper er.[111]

Kjøper har anledning til å legge flere vouchers inn i en *wallet.* Her vil det være krav til registrering tilsvarende andre wallets, som beskrevet over. Det vil være naturlig å kontakte tjenestetilbyder for informasjon om bruker og transaksjoner.

---

[109] Forutsetter her at wallet-tilbyder er utenlandsk.
[110] Om vouchers – se Kapittel 1: Beskrivelse av nyere betalingstjenester – Internettbaserte betalingstjenester - Vouchers
[111] Forutsetter at kort er benyttet ved kjøp av vouchers

Betalingsformidler

Betalingsformidlere kjennetegnes ved at de mottar midler fra avsender, for så å overføre dem til mottaker i utlandet gjennom sitt betalingsnettverk. Hvis overføringen fra avsender til betalingsformidler skjer fra ordinær bankkonto, vil transaksjonen fremgå av avsenders kontoutskrift. Det vil ikke fremgå av kontoutskriften hvem endelig mottaker er.

Betalingsformidler mottar midlene og overfører i betalingsformidlers navn til mottaker i utlandet. Utenlandske betalingsformidlere disponerer ofte en norsk bankkonto, som pengene rutes til først. Transaksjonen vil fremgå av valutaregisteret med betalingsformidler som avsender, og mottaker i utlandet kan her være identifisert. Noen betalingsformidlere har imidlertid som praksis å samle flere transaksjoner i én overføring fra betalingsformidlers konto i Norge til betalingsformidlers konto i utlandet, før de fordeles til de respektive mottakere. I slike tilfeller vil ikke transaksjoner som betalingsformidler foretar på brukers vegne kunne identifiseres gjennom valutaregisteret. Betalingsformidlerens bankforbindelse i Norge vil heller ikke ha opplysninger som kan oppklare forhold rundt transaksjonen.

Betalingsformidler/tjenestetilbyder vil i de fleste tilfeller ha opplysninger om bruker og hele transaksjonskjeden.

Det eksisterer aktører som tilbyr betalingsformidling for kunder uten å ha eget betalingsnettverk. Betalingsformidlere engasjeres da til å foreta selve overføringen. I slike tilfeller vil heller ikke betalingsformidleren ha informasjon om hvem som er avsender og mottaker av transaksjonen. I valutaregisteret vil kun aktøren være identifisert. For å kartlegge transaksjonskjeden må henvendelse rettes til aktøren som har kundeforholdet til bruker.

Tredjepartstilbyder

Et kjennetegn ved tredjepartstilbydere er at de initierer betaling fra konto, men pengene går ikke *via* tilbyderen. Transaksjonen vil fremgå av brukers kontoutskrift, men det er opp til tilbyderen hvor mye informasjon om transaksjonen som meddeles banken. I avsenders kontoutskrift og underbilag vil det *ikke* fremgå informasjon om mottaker av transaksjonen. I mottakers kontoutskrift vil avsender fremgå.

Dersom transaksjonen er grensekryssende vil transaksjonen fremgå av valutaregisteret som en ordinær bank- eller korttransaksjon.

Tjenestetilbyder vil være den som i størst grad har oversikt over bruker og gjennomførte transaksjoner.

Faktureringstjenester

Fakturering som betalingstjeneste er ikke et nytt fenomen. Det som er nytt er at en aktør som ikke er part i handelen tar på seg oppdraget med å fakturere kunden. På denne måten vil ikke butikken ha informasjon om kunden (utover eventuelt leveringsadresse), og kundens betalingstjeneste vil ikke ha informasjon om handelen.[112] Transaksjonen vil altså fremgå av for eksempel kundens kontoutskrift, men uten informasjon om hvor det er handlet.

[112] Med "kundens betalingstjeneste" menes måten kunden velger å betale fakturaen på

Tjenestetilbyder er den som har informasjon om hele transaksjonskjeden, i tillegg til bruker. Tilbyder vil ha kunnskap om bruker for å kunne fakturere vedkommende, samt kunnskap om fakturagrunnlaget, eller i det minste hvor handelen er gjort.

Mobile betalingstjenester

Ved bruk av mobile betalingstjenester gir brukers kontoutskrift fullstendig informasjon om transaksjonen forutsatt at brukeren har konto hos banken som tilbyr tjenesten. Eksempelvis vil kontoutskrift fra en kunde i DNB som benytter seg av tjenesten VIPPS, gi informasjon om hvem pengene er overført til og fra. Kontoutskrifter fra andre banker vil ikke gi denne informasjonen, fordi transaksjonen først går til DNB. Typisk for dette eksemplet vil være en kunde hos Nordea som benytter seg av VIPPS, vil kontoutskriften kun inneholde «VIPPS by DNB», som informasjon om transaksjonen samt beløp og dato for transaksjon. Kundens eventuelle angivelse av hva beløpet gjelder fremkommer ikke av kontoutskriften.

For å innhente informasjon om transaksjon med mobile betalingstjenester kan banken som har hovedsamarbeid med tjenesten kontaktes.

At utenlandske aktører etterhvert får anledning til å tilby mobile betalingstjenester i Norge, medfører at politi- og kontrolletatene må til utlandet for å få tilstrekkelig informasjon om transaksjonene.

Virtuell valuta

Kryptovalutaens blockchain ligger åpent på nett. Hvor mye informasjon som er lesbart fra de ulike blockchainene varierer for de ulike kryptovalutaene. For Bitcoin ligger offentlige nøkler åpent på blockchain, men det er ikke mulig å lese av dette hvem som eier de offentlige nøklene.[113] Med analyseprogram er det imidlertid mulig å kartlegge transaksjonshistorikken for en offentlig nøkkel / bitcoin-adresse, men for å avdekke *brukeren* er det behov for konkret informasjon om hvem som innehar den private nøkkelen.[114] [115]

De private nøklene oppbevares i wallets på nett, lokalt på datamaskinen, på minnepinne eller skrevet ned på papir.[116] Informasjon om private nøkler er helt avgjørende for å knytte transaksjoner til bruker.

Av valutaregisteret fremgår valutatransaksjoner mellom Norge og kjente vekslere av virtuell valuta i utlandet.

Det er ikke tilsvarende mulighet til å se veksling mellom to norske parter (lokale kjøpere/selgere), og det er heller ikke mulig å se veksling fra en kryptovaluta til en annen. Analyse fra flere ulike kilder gir grunnlag for å si at overvekten av kjøp og salg av virtuell valuta skjer fra person til person, og ikke gjennom utenlandske vekslingsbørser.

---

[113] Om offentlig nøkkel – se Kapittel 1: Beskrivelse av nyere betalingstjenester – Virtuell valuta
[114] Eksempler på analyseprogram er Walletexplorer.com og www.chainalysis.com
[115] Om privat nøkkel – se Kapittel 1: Beskrivelse av nyere betalingstjenester – Virtuell valuta
[116] Varme og kalde wallets ref. beskrivelse i Kapittel 1: Beskrivelse av nyere betalingstjenester – Virtuell valuta

Enkelte aktører som tilbyr bitcoin-wallets, tilbyr også betalingskort knyttet til walleten. Der disse kortene blir benyttet i Norge, vil innløser rapportere transaksjonen til valutaregisteret på lik linje med andre utenlandske kort benyttet i Norge.[117]

Ved bruk av bankkonto i forbindelse med veksling av virtuell valuta med vekslingsbørser, kan underbilag til kontoutskriften gi informasjon om avsender/mottaker.

Hvilke hindre står kontrolletatene overfor

Selv om tradisjonelle og nyere betalingstjenester er sporbare, har politi- og kontrolletatene flere utfordringer knyttet til sporene. Kriminelle som benytter seg av nyere betalingstjenester i den hensikt å begå økonomisk kriminalitet, ønsker å tilsløre transaksjonen. Flere av tjenestene profilerer seg med å være egnet til å skjule spor, og enkle å ta i bruk.

Noen av hindrene kan være så store at identifisering av bruker blir vanskelig.

Kryptering

«Kryptering er en matematisk metode som sørger for konfidensialitet ved at informasjonen ikke kan leses av uvedkommende»[118]

Kryptering finnes i flere former og er integrert i bruk eller kommer ved eksternt behov. Integrert kryptering finnes ved bruk av telefon eller ved programmer som har integrert kryptering.

Ekstern kryptering er lettvint å tilegne seg og benyttes normalt sammen med en datamaskin. Dekryptering er avhengig av riktig verktøy og passord/nøkkel for å få tilgang til informasjon. Uten dekryptering vil informasjonen være uleselig.

Mellomtjenere og Virtuelle Private Nettverk (VPN)

Kriminelle benytter seg av tilleggstjenester som mellomtjener og VPN for å skjule IP-adresse.

Mellomtjener er en ekstern server/datamaskin som mottar informasjon om søket, og endrer IP-adressen og utfører søket. Når tjenesten har utført søket, vil den svare tilbake om hva den fikk av informasjon. Tjenesten som mottok søket, ser ikke den reelle IP-adressen, men en IP-adressen fra mellomtjeneren.

Tjenesten er ikke kryptert og kan overvåkes av internettleverandører (for eksempel Telenor, Get). Tjenesten brukes ofte for å kunne se innhold i nettsider som er begrenset til landets godkjente IP-adresser. Eksempelvis har enkelte nettsider innhold som er begrenset til brukere i USA. Gjennom en mellomtjener i USA, vil det være mulig å se denne fra andre land.

---

[117] Forutsetter her utenlandske wallet-providers
[118] www.datatilsynet.no Kryptering av informasjon

Virtuelt Privat Nettverk (VPN) er en tjeneste som skaper punkt-til-punkt forbindelse i form av en tunell gjennom andre nettverk. I likhet med mellomtjener endrer VPN IP-adressen til brukeren. Det finnes flere typer VPN og i ulike former. Det mest vanlige er å bruke kryptert VPN, som krypterer alt av informasjon fra bruker til VPN serveren. Nettleverandøren kan se at brukeren benytter seg av VPN, men ikke innholdet. Tilbydere av VPN er de som har informasjon om reell IP-adresse fra bruker.

Grunnlaget er at brukeren har installert et VPN-program på en datamaskin, som krypterer informasjonen frem til VPN-serveren. Nettverksleverandøren vil kun se kryptert informasjon. Tjenesten er fleksibel ved at brukeren kan velge hvilket land som IP-adresse skal endres i, og om IP-adressen skal endres i flere land.

Utfordringene med tjenestene er at enkelte tilbydere er anonyme (hverken telefonnummer eller kontaktpunkt), eller at de ikke svarer på henvendelser.

Darkweb, Darknet og Tor-nettleser

Darkweb er nettsider som ikke er tilgjengelig ved indekserte søk ved bruk av søkemotorer som Google og kan være er alt fra hjemmenettverk til websider.[119]

Darknet er nettsteder som krever egne programmer for å få tilgang, slik som TOR-nettleser. Ved bruk av programvare kan det på en enkel måte gis tilgang til nettsider som tilbyr kjøp og salg av ulike ulovlige varer eller tjenester.

Bruk av Darknet i kombinasjon med eksempelvis TOR, vanskeliggjør sporbarheten av brukere.

TOR er en nettleser som enkelt kan lastes ned fra nettet i likhet med nettlesere som Firefox, Chrome og Opera. Det som gjør denne nettleseren unik, er at den gir tilgang til «.onion»-domener, som er lenker primært benyttet i Darknet.[120]

Eksempel på en adresse er: http://reloadedudjtjvxr.onion (Silkroad v3.0).

Noen adresser er åpne for alle som benytter seg av TOR, andre er lukkede i form av at brukeren må ha invitasjon/godkjenning fra andre brukere for å kunne se innholdet på nettsiden. Det finnes flere TOR «noder» i verden som trafikken rutes igjennom.[121] [122] Internt i TOR nettverket er det ende-til-ende kryptering. Dette innebærer at all trafikk som rutes gjennom TOR nettverket er anonymt. Alle søk i TOR-nettverket går av sikkerhetsmessige grunner igjennom minimum tre noder. Det er ingen systematikk i hvilke noder trafikken rutes gjennom.

Hvis det benyttes TOR nettleser for å besøke domener som er tilgjengelig på «det åpne nettet», må brukeren bryte ut av TOR nettverket.[123] Dette gjøres fra en «exit node», og

---

[119] Indekserte søk – en prosess som ordner et sett med data/informasjon etter søk.
[120] .onion er et domenesuffiks i likhet med .no og .com.
[122] Det er 3 noder i TOR-nettverket; mellom-node, exit-node og bro-noder. Nodene har forskjellig funksjoner, men er med på å gi datakraft til nettverket.
[122] For mer informasjon om nettverkstrafikken, se https://torflow.uncharted.software
[123] Åpne nettet brukes i sammenheng med lenker som er tilgjengelig ved normalt bruk av internett.

domenet som besøkes vil kunne se IP-adressen. Om en bruker befinner seg i Oslo og besøker eksempelvis www.DN.no ved bruk av TOR, kan domenet få informasjon om at brukerens plassering er i England. Domenet vil ikke få informasjon om brukerens reelle IP-adresse, kun exit nodens IP-adresse.

Anonymiteten kan imidlertid brytes ved at brukeren gjør en feil som for eksempel å lekke informasjon om Domain Name System (DNS) tilknyttet IP-adressen til domenet.[124]

[124] Lekkasje i Domain Name System (DNS) fører til at domener får informasjon om hvilken internettleverandør du benytter.

Kapittel 3: Bruk av nyere betalingstjenester ved utøvelse av økonomisk kriminalitet

Straffesaksdokumenter og dommer er innhentet fra flere politidistrikt og særorgan for å se bruken av nyere betalingstjenester i sammenheng med kriminalitet i Norge. Foruten politiets egne saker er anmeldelsene hovedsakelig inngitt av Skatteetaten og Tolletaten.

Sakene som er analysert omhandler hvitvasking, bedragerier, skjult formue, skatteunndragelse, heleri, narkotikakriminalitet, dokumentforfalskning og seksualforbrytelser.

Drivere

Kriminelle har behov for å utføre anonyme og sikre betalinger.[125] Noen betalingssystemer er godt tilpasset et slikt formål, spesielt i kombinasjon med sekundære tjenester, som for eksempel bitcointransaksjoner i kombinasjon med Darknet.

Kunnskapen om politi- og kontrolletatenes muligheter for å spore brukere deles villig mellom de kriminelle.[126] Kunnskapen blir distribuert på det åpne og lukkede nettet, for at flere kan benytte systemer og tjenester som ikke legger spor.

Anonymitet er den viktigste driveren for bruk av slike tjenester i forbindelse med økonomisk kriminalitet. Enkelte tjenester krever få eller ingen personopplysninger ved opprettelse av kundeforhold. Det følger begrenset informasjon med transaksjonene. Tjenestetilbyderne er ikke rapporteringspliktige til norske myndigheter etter hvitvaskingsregelverket.

Tjenesten må kunne fullføre betalinger raskt og sikkert og inneha få eller ingen begrensninger i transaksjonsnettverket. Flere tjenester overskrider beløpsgrenser og reklamerer for sekretesse.

[125] iOCTA 2016 s 42
[126] https://99bitcoins.com/ Complete guide using bitcoin anonymously

Videre må tjenesten være tilgjengelig i store deler av verden og være brukervennlig.

Omfang

Bruk av nyere betalingstjenester ved utøvelse av økonomisk kriminalitet er økende i omfang og kompleksitet. Utviklingen sees i klar sammenheng med at tilbydere av slike tjenester har økt betraktelig og er lettere tilgjengelig enn tidligere. Informasjon i registre og antall straffesaker indikerer også at nyere betalingstjenester benyttes oftere vedrørende økonomisk og annen profittmotivert kriminalitet.

Valutaregisteret indikerer også økning i bruk av nyere betalingstjenester. Ved reguleringsendringer om forbud til banker om innførsel-/utførsel av valuta til ulike tjenester, viser valutaregisteret at brukermassen forflytter seg til en annen tjeneste.

Etatenes begrensede muligheter til å avdekke slike transaksjoner tilsier at mørketallene knyttet til bruk av nyere betalingstjenester er store.

Saker med virtuell valuta

I saker med bruk av virtuell valuta, ble det kun gitt informasjon om straffesaker vedrørende kryptovaluta. Straffesaksdokumentene vedrørende bruk av kryptovaluta dreier seg hovedsakelig om tilegnelse av ulovlige varer og økonomisk utbytte av en straffbar handling.

Ulovlige varer som typisk kjøpes ved hjelp av kryptovaluta er narkotika, falske pass, identitetsdokumenter, og førerkort og falske penger. Slike varer er enkelt tilgjengelig på Darknet.

Et trekk i samtlige saker er at kjøpere og selgere benytter seg av nettleseren TOR, som gir tilgang til det mørke nettet.

Beslag og informasjonen fra speiling av datamaskiner og harddisker er begrenset, men i noen tilfeller har beslaget vist spor av lenker som er benyttet i TOR.[127] I saker hvor TOR brukes riktig, vil ikke denne informasjonen være tilgjengelig ved beslag, siden TOR er designet til ikke å etterlate søkerhistorikk.[128]

I alvorlige saker har politiet i enkelte tilfeller lyktes med å ta beslag i kryptovalutaens wallet (der kryptovalutaen er lagret). I mindre alvorlige saker prioriteres fortrinnsvis primærforbrytelsen i etterforskingen, og det gjøres som regel ikke beslag av konti tilknyttet kryptovalutaen som inneholder utbyttet fra det straffbare forholdet.

I mindre alvorlige saker relatert til Bitcoins er politiet avhengig av godt samarbeid fra siktede/mistenkte, for å knytte gjerningspersonen til primærlovbruddet. Risikoen ved å støtte seg på informasjon fra siktede/mistenkte er tilsløring av andre konti med gjenstående verdi.

---

[127] Det som kan ha betydning som bevis, kan beslaglegges jf. straffeprosessloven § 203

[128] Det finnes instruksjoner på internett om riktig bruk av TOR, ved å unngå bruk av Windows, deaktivere Java, se for øvrig note 121.

Kriminelle kombinerer ofte ulike tjenester. Ett modus er å veksle kryptovaluta hos utenlandske vekslere, for så å overføre til en utenlandsk konto eller et forhåndsbetalt kort i fiktivt navn som kan benyttes i Norge og verden forøvrig.
Kryptovaluta kan veksles fra store utenlandske vekslere som Kraken, Bitstamp eller norske lokale vekslere til reell valuta. Midlene overføres til egen bankkonto, utenlandske bankkonti eller forhåndsbetalte kort som kan brukes i Norge.

Saker med internettbaserte betalingstjenester

Et flertall av straffesakene er relatert til bruk av internettbaserte betalingstjenester.

Internettbaserte betalingstjenester er i hovedsak brukt for å forflytte penger raskt. Kontoutskrifter viser at internettbaserte betalingstjenester er benyttet, men hverken i kontoutskriftene eller valutaregisteret framkommer det hvem pengene er overført til eller fra. Erfaringer tilsier at selv ikke betalingstjenesten kan gi informasjon om hvor pengene er overført til. Det de kan henvise til er hvem som har overført eller hvilket foretak som har overført pengene.

I straffesaker med betydelige beløp kan det sendes anmodning fra politiet om utlevering av opplysninger fra betalingsformidleren. Erfaringer tilsier at det kan ta alt fra én måned til halvannet år før henvendelsen blir besvart, og variasjonen fra land til land er stor. Anmodninger til betalingstjenester i Europa og enkelte andre land besvares innen tre måneder, mens det i land som USA vil kunne ta opp mot halvannet år.

Straffesakene viser følgende:

- I saker med lavt beløp sendes ikke rettsanmodning til utlandet for å følge penger eller andre spor. Sakene kan også bli henlagt fordi det ikke anses hensiktsmessig å bruke ressurser på internasjonal etterforsking.
- Når grunnlaget er til stede er det svært effektivt å fryse konti (spesielt tradisjonelle). Denne metoden er rask og effektiv for å sikre verdien i utlandet og fungerer effektivt i en tidlig fase i etterforskingen. Hastigheten transaksjonene utføres i gjør det imidlertid utfordrende å stanse en pågående transaksjon.
- Transaksjonseier må kunne identifiseres for å innhente ønskede opplysninger om transaksjoner. Komplekse organisasjonsstrukturer internasjonalt gjør det ofte utfordrende å finne korrekt kontaktpunkt hos tjenestetilbyder.
- Internettbaserte betalingstjenester benyttes oftest til å overføre store beløp over tid til spillselskaper. Det anmodes i varierende grad om innsyn i spillesaldo på nett for å se videre bruk av pengene.
- Internettbaserte betalingstjenester brukes i kombinasjon med andre typer betalingstjenester til å overføre penger ut av Norge til ukjent konti.
- Internettbaserte betalingstjenester er benyttet som betalingsmetode ved videooverføring av seksuallovbrudd. Tjenestene behandler overføringen raskt og mottaker kan verifisere mottak av penger i løpet av få sekunder. Trenden er økende.

[129]

Saker med forhåndsbetalte kort

De norske forhåndsbetalte kortene er begrenset i beløpsstørrelse, og dette har en påvirkning på omfanget av den økonomiske kriminaliteten i straffesaker. Norske forhåndsbetalte kort benyttes for å tilsløre den økonomiske gevinsten og hvitvaske utbytte fra den kriminelle handlingen.

[129] Med kontaktpunkt menes personer hos tilbydere som kan motta henvendelser fra offentlige myndigheter

Norske og utenlandske forhåndsbetalte kort benyttes i mange former for kriminalitet, men er mest utbredt i saker som omhandler:

- Narkotikakriminalitet (Ved kjøp/salg)
- Skjult inntekt og formue i utlandet
- Hvitvasking av:
    - Skattesvik
    - Heleri
    - Ran
    - Bedrageri
    - Tyveri
- Tilsløre reise:
    - Hoteller
    - Bensinstasjoner
    - Kjøp i butikk
- Hallikvirksomhet
- Arbeidslivskriminalitet:
    - Svart arbeid
    - Svart omsetning
    - Utbetaling av lønn

Det foreligger få straffesaker hvor utenlandske forhåndsbetalte kort er brukt til lovstridige formål. Dette kan skyldes at det er utfordrende for etatene å skille mellom tradisjonelle utenlandske bankkort og forhåndsbetalte. Det er krevende å kartlegge gjentakende bruk av utenlandske forhåndsbetalte kort brukt i Norge.

Det gjennomgående i sakene som er innhentet er at de omhandler hvitvasking av betydelige beløp. Ofte har innehaver forhåndsbetalte kort i utlandet flere kort i samme bank, slik at uttaksbegrensninger på kortene utnyttes.

I straffesaker er eier av kortene ofte ikke personen som reelt bruker kortet. Kortene står gjerne oppført på et foretak eller en falsk identitet.

Saker med mobile betalingstjenester

Det foreligger få straffesaker knyttet til mobile betalingstjenester. Informasjon og saker omhandler små bedragerier eller kjøp/salg av ulovlige varer. Tjenesten som har blitt benyttet er VIPPS.

Kapittel 4: Politi- og kontrolletatenes erfaringer med nyere betalingstjenester

Etatenes forhold til nyere betalingstjenester

NTAES har innhentet informasjon fra relevante miljøer i hver etat, og samlet informasjon om hvilken kompetanse de opplever å ha på området nyere betalingstjenester, hvordan nyere betalingstjenester berører etatenes kontrollarbeid, og hvilke erfaringer de har fra saker hvor nyere betalingstjenester er benyttet.

Etatene har svært ulike erfaringer med bruk av nyere betalingstjenester. Etatene har også ulik opplevelse av hvorvidt pengestrømmer gjennom slike betalingstjenester angår deres arbeid.

Arbeidstilsynet er den etat som i minst grad opplever at bruk av nyere betalingstjenester er utfordrende for deres arbeid. De beskriver i ett tilfelle å ha erfart at forhåndsbetalt kort ble benyttet som lønnsutbetaling med det formål å unngå beskatning, men ser forøvrig ikke bruk av nyere betalingstjenester som svært relevant. De er imidlertid av den oppfatning at deres økte oppmerksomhet på området kan bidra til innsamling av informasjon som kan nyttiggjøres av de øvrige etatene i samarbeidet mot arbeidslivskriminalitet.

NAV Kontroll har varierende kjennskap til nyere betalingstjenester, men noen enheter beskriver utfordringer med slike transaksjoner gjennom sitt arbeid. Det er gjerne ved undersøkelser som knytter seg til skjult lønn og arbeidsaktivitet at transaksjoner gjennom nyere betalingstjenester identifiseres. Erfaringer som trekkes frem er transaksjoner relatert til nettspill, og saker der næringsdrivende tar imot bestillinger- og tar seg betalt gjennom nettbaserte tjenester.

NAV Kontroll har imidlertid ikke hjemmel til å innhente opplysninger fra utenlandske tjenestetilbydere.

Tolletaten har kunnskap om betalinger gjennom nyere betalingstjenester gjennom to av sine fagområder. Dette er ved fastsettelse og kontroll av tollverdi på deklarerte

varer, hvor kunden blir bedt om å dokumentere beløpet, og ved etterretning på ulovlig vareførsel. Tolletaten ser at nyere betalingstjenester brukes for kjøp av alle typer varer, og særlig ved betaling for ulovlige varer.

Kontrollavdelingen Tolldirektoratet (TOD) har noe kompetanse på virtuell valuta, mens det i tollregionene er spredt kompetanse på enkelte betalingsformer som er tilegnet gjennom saker. Det er ønskelig å bygge et kompetansemiljø på nyere betalingstjenester i Tolletatens Etterretningssenter (TES) som ble etablert 15. februar 2017. Tolletaten peker på at det i etterretningsøyemed er viktig å kunne identifisere betaler og mottaker. Økt kompetanse om nyere betalingstjenester vil også medføre at kontroll av tollverdi kan utføres mer effektivt.

Skatteetaten har avdekket bruk av nyere betalingstjenester gjennom kontroller på områdene netthandel, nettgambling og bloggere, samt ved kontroll av skattepliktige med skjult formue i utlandet.

Skatteetatens kunnskap om nyere betalingstjenester er i stor grad opparbeidet gjennom Riksprosjekt E-handels kontroller og analyser. Riksprosjektet var, inntil det ble avsluttet 31.1.2017, en landsdekkende satsning i Skatteetaten, med formål å bidra til økt etterlevelse av skatte- og avgiftsregelverket innenfor elektronisk handel (e-handel). Arbeidet var organisert i ulike delprosjekter, hvor kunnskap om nyere betalingstjenester primært ble generert i delprosjektene netthandel, nettgambling og sosiale medier/blogg.

Digitalt Utviklings- og Kompetansesenter (DUKS) i Skatt øst ble fra 1.1.2017 slått sammen med Riksprosjekt E-handels tekniske senter (TC) i Skatt nord, som sammen dannet den nye nasjonale enheten SIDU – Senter for internettgranskning og digital utvikling.[130] [131] Her vil kompetansen på området nyere betalingstjenester videreutvikles. SIDU skal yte bistand til kontrollmiljøene i etaten samt bistå miljøet i SAES (Sikring Analyse av Elektroniske Spor) med speiling av data, og IT-revisorer til kartlegging av datasystemer/regnskapssystemer.

Kunnskap om bruk av utenlandske kort i Norge, herunder forhåndsbetalte kort, er i stor grad opparbeidet gjennom Prosjekt Internasjonale Pengetransaksjoner (PIP). PIP-prosjektet har som mål å avdekke skjult inntekt og formue i utlandet ved å avdekke mistenkelige pengetransaksjoner over landegrensene.

Miljøene NTAES har vært i kontakt med oppgir at de har god kompetanse på området, men at en forutsetning for å opprettholde kompetansen er at saksbehandlerne får fortsette å kontrollere denne typen saker. En generell kompetanseheving i etaten på området vil føre til økt bevissthet om nyere betalingstjenester. Dette vil bidra til at flere i kontrollmiljøene vil være i stand til å følge pengesporet i sakene.

---

[130] DUKS hadde ansvar for utvikling av digital kompetanse i Skatt øst, og jobbet blant annet med innhenting av informasjon fra internett og å følge med på trender innen den digitale økonomien. En sentral oppgave var å yte bistand til kontrollmiljøene.

[131] Teknisk senter (TC) var en del av Riksprosjekt e-handel, med fokusoppgaver knyttet til utplukk av kontrollobjekter, kompetanseutvikling og kartlegging av trender. Enheten utviklet ekspertise innen innhenting av informasjon fra åpne kilder.

Politiet ser bruk av nyere betalingstjenester i et bredt spekter av saker, for eksempel i narkotikakriminalitet, overgrepssaker, hvitvasking, samt en rekke former for profittmotivert kriminalitet; underslag, bedrageri, økonomisk utroskap, skatteunndragelse, kreditorunndragelse mv.

Hos **øko-teamene** i politiet synes kunnskap om nyere betalingstjenester å være fragmentert og basert på enkeltsaker hos etterforskere. Teamene har begrenset tilgang på teknisk kompetanse som kan bistå etterforskere i å forfølge elektroniske spor lokalt. I alvorlige saker har de mulighet til å be om bistand fra Kripos eller ØKOKRIM. Unntaket er Finans og miljø ved Oslo politidistrikt som har egen datateknisk og datataktisk avdeling som bistår ved behov.

Teamene beskriver en rekke fordeler ved økt kunnskap om nyere betalingstjenester. Etterforskere vil i større grad kunne følge pengespor, identifisere hvor pengene kommer fra, og avdekke hvem som disponerer betalingstjenestene. Økte muligheter for å identifisere bakmenn, avdekke ytterligere straffbare forhold, og sikring og inndragning av verdier, oppleves også som en potensiell gevinst ved kunnskapsheving. Økt kunnskap om nyere betalingstjenester kan gi bedre kvalitet i etterforskingen, og bidra til større utnyttelse av informasjonen man får under etterforskingen.

Ved **ØKOKRIM** ligger kunnskap om hvordan nyere betalingstjenester kan benyttes som verktøy for hvitvasking og annen økonomisk kriminalitet i hovedsak hos Enheten for Finansiell Etterretning (EFE). EFE behandler rapporter om mistenkelige transaksjoner (MT-rapporter) som sendes inn av rapporteringspliktige etter hvitvaskingsregelverket.

MT-rapporter som vedrører nyere betalingstjenester gjelder i all hovedsak transaksjoner i tilknytning til nettspill, som mistenkes å dreie seg om hvitvasking, og bruk av bitcoins i forbindelse med omsetning av narkotika. EFE får også rapporter på transaksjoner knyttet til kjøp og bruk av forhåndsbetalte kort.

For EFE vil økt kompetanse om nyere betalingstjenester bidra til mer presise analyser av finansielle spor, samt være nyttig i veiledningsøyemed overfor politi og kontrollmyndigheter. I ØKOKRIM har NTAES også vært i kontakt med Avdeling 3 (Utbytte, hvitvasking-, og bistandsteamet), som har tilegnet seg kunnskap om nyere betalingstjenester gjennom noen enkeltsaker. Avdeling 3 understreker viktigheten av at erfaringer fra innhenting av opplysninger og dokumentasjon deles. Da kan informasjonen benyttes i kommende saker med kunnskap om hvilke tiltak som er mest effektive for å fremskaffe dokumentasjon, og sende formell henvendelse til riktig sted. Økt kompetanse på området sikrer at effektive etterforskingsskritt kan iverksettes i en tidlig fase, slik at eier av verdiene raskt kan spores opp, og verdiene eventuelt kan sikres.

Ved **Kripos** har seksjon for internettrelatert etterforskingsstøtte (IRES), avdeling for teknologi og operative tjenester, opparbeidet kunnskap om nyere betalingstjenester gjennom bistand i interne saker på Kripos og i bistandssaker til distriktene. Seksjonen har både teknisk og taktisk kompetanse på kryptovaluta.[132] Det finnes også teknisk kompetanse på kryptovaluta på seksjon for elektroniske spor (ESPOR), og økonomisk etterforskingskompetanse på seksjon for organisert kriminalitet (ORGKRIM).

[132] Om kryptovaluta, se Kapittel 1: Beskrivelse av nyere betalingstjenester – Virtuell valuta

Kripos' erfaringer med nyere betalingstjenester gjelder i stor grad bruk av kryptovaluta til kjøp av ulovlige varer og tjenester, gjerne i kombinasjon med hvitvasking ved bruk av ulike internettbaserte betalingstjenester, og uttak av utbytte ved bruk av forhåndsbetalte kort. Sakene har ofte sin opprinnelse på det mørke nettet. Kripos har med sin tekniske kompetanse gode forutsetninger for å følge spor tilknyttet nyere betalingstjenester. Fagmiljøene på Kripos har et godt grunnlag for å tilegne seg nødvendig kompetanse etter hvert som utfordringene med nyere betalingstjenester øker i konkrete straffesaker. Økt kompetanse om type spor fra nyere betalingstjenester kan utnyttes til å spore pengestrømmer, knytte personer til transaksjoner og avdekke kriminelle nettverk.

Nærmere om etatenes erfaringer

Arbeidstilsynet

Arbeidstilsynets erfaringer med nyere betalingstjenester begrenser seg til funn av forhåndsbetalte kort benyttet som lønnsutbetaling.

NAV Kontroll

NAV Kontroll har gjennom sine saker sett bruk av forhåndsbetalte kort, mobile betalingstjenester, og internettbaserte betalingstjenester. Eksempelvis har NAV sett innbetalinger på konto fra internettbaserte betalingstjenester. Innhentede underbilag gir ikke informasjon som kan oppklare midlenes opprinnelse. Dette mistenkes i hovedsak å dreie seg om nettspill.

Et annet eksempel på saker som synes å gå igjen, er der et foretak eller en person driver en netthandel med kjøp og salg av varer, og kundene betaler og bestiller via PayPal. Dette ser man ingen spor av, før det etter en tid overføres et eller flere store beløp fra PayPal-konto inn på bankkonto. NAV Kontroll har i slike tilfeller ingen mulighet til å kartlegge omfanget av salget som foregår i netthandelen.

NAV Kontroll har hjemmel til å hente inn opplysninger fra norske finansinstitusjoner gjennom Folketrygdloven § 21-4. NAV har tradisjonelt kun forholdt seg til norske banker og kredittselskaper i denne type saker.

Medarbeidere i NAV Kontroll er av den oppfatning at antall saker hvor nyere betalingstjenester benyttes er økende i deres portefølje, men kontrollarbeidet begrenses av det som oppleves som svært begrensede muligheter til å innhente opplysninger fra aktuelle tredjeparter.

Tolletaten

Tolletaten har gjort seg erfaringer med de fleste typer nyere betalingstjenester gjennom sitt arbeid. Reisende har blitt stoppet med forhåndsbetalte kort, sannsynligvis oftest i lovlig ærend. Kortene anses imidlertid som egnet middel til å smugle valuta, og har også blitt brukt til innkjøp av ulovlige varer.

Ved fastsettelse av tollverdi for lovlige varer, blir kunden bedt om å dokumentere beløpet. Det har i tilfeller vært lagt fram utskrift fra PayPal-konto og dokumentasjon for pris i bitcoins.

Når det gjelder betaling for ulovlige varer skjer kjøp over internett både med Bitcoin, forhåndsbetalte kort, PayPal, Earthport og andre internettbaserte betalingstjenester. Nyere betalingstjenester brukes for kjøp av alle typer varer, og identifiseres gjennom tilbakemeldinger fra kjøper og faktura/korrespondanse kjøper har hatt.

Tolletatens erfaring er at av nyere betalingstjenester er PayPal oftest brukt ved handel av lovlige varer over internett. For ulovlige varer er det oftest Bitcoin eller andre virtuelle valutaer som benyttes.

Tolletaten innhenter hovedsakelig ikke opplysninger fra tilbydere av nyere betalingstjenester. Dette har sin bakgrunn i at Tolletaten som regel får opplysningene fra importørene frivillig og med plikt til å avgi informasjon i henhold til tolloven. Dersom kjøpesummen ikke lar seg dokumentere hjemler tolloven at tollverdi kan fastsettes på andre måter, blant annet ut fra pris på identiske eller lignende varer som er innført tidligere.

Tolletaten utveksler regelmessig etterretningsinformasjon med andre etater, og da særlig politiet og Skatteetaten. Det har blant annet vært et samarbeid med Kripos om hvitvasking som involverer narkotikaomsetning og Bitcoin. Tolletaten erfarer at det generelt tilkommer begrenset med informasjon tilbake fra andre etater.

Tolletaten deltar i aksjoner i regi av World Customs Organization (WCO). Aksjonene involverer tidvis også nyere betalingstjenester. I noen tilfeller deltar store private aktører som for eksempel PayPal.

Tolletaten har samarbeidsavtaler med land i hele EØS-området og en rekke andre viktige handelspartnere. Samarbeid med utenlandske tollmyndigheter har vært, og vil være et svært viktig element når det gjelder å avdekke smugling, ulovlige varer og uriktige tollverdier.

Økt bruk av betalingsmåter hvor transaksjonen ikke fremgår av valutaregisteret vil innebære større utfordringer med å avdekke smugling av varer gjennom etterkontroll. Det vil også berøre etterretningsarbeidet knyttet til kjøp av ulovlige varer, idet penger i større grad beveger seg over landegrensen uten å legge igjen spor, og uten at kontanter må fysisk smugles over grensen. Videre gjør bruk av digital valuta det mer utfordrende å spore kjøpere og selgere av ulovlige varer på nett, og det vil kreve økt kompetanse for å holde tritt med dette.

Skatteetaten

Skatteetaten har gjennom satsningen på e-handelsområdet sett bruk av forhåndsbetalte kort primært i forbindelse med nettspill. De ser også at internettbaserte betalingstjenester i stor grad benyttes til å gjøre innskudd hos utenlandske spillselskap, dette uten at den norske spilleren nødvendigvis har et bevisst forhold til tredjeparten. Det er også identifisert tilfeller med overføring fra spillkonto til spillkonto.

Skatteetaten har også erfaringer med bruk av PayPal som betalingstjeneste, hvor eier av nettbutikk tar betalt via PayPal. De har sett tilfeller av at midlene blir stående på PayPal-kontoen, hvorpå omsetningen helt eller delvis unndras beskatning i Norge.

Skatteetaten anser PayPal for å være den største aktøren for betalingsformidling ved netthandel i Norge, men ser at også Klarna i økende grad benyttes.

Når det gjelder virtuell valuta er Skatteetatens erfaring at Bitcoin ikke er særlig utbredt som betalingsløsning i Norge i dag. De har erfart at brukersteder som skriver at de tar betalt i Bitcoin allikevel ikke har hatt teknologien ferdig.

Innhenting

Hjemmel til innhenting av opplysninger fra betalingstjenestetilbydere i Norge følger av skatteforvaltningsloven og merverdiavgiftsloven:

- Tredjeparts plikt til å gi opplysninger etter krav følger av skatteforvaltningsloven §§ 10-2 til 10-6 og merverdiavgiftsloven §§ 16-2 til 16-5.
- Skattemyndighetenes adgang til å foreta kontrollundersøkelser hos skattepliktig og tredjepart følger av skatteforvaltningsloven § 10-4 og merverdiavgiftsloven § 16-6.

Skattemyndighetene har også mulighet til å foreta målrettet kontroll, det vil si innhente tredjepartsopplysninger på ikke navngitte skattepliktige og bruke opplysningene for å kunne identifisere kontrollobjekter. Med kontrollhjemlene i skatteforvaltningsloven § 10-2 første ledd og merverdiavgiftsloven § 16-2 første ledd er tredjeparts opplysningsplikt ikke begrenset til bestemte transaksjoner eller navngitte aktører.

For innhenting fra utlandet benyttes bistandsanmodninger som sendes via kompetent myndighet. Hjemmel for innhenting av opplysninger fra utlandet følger av skatteavtaler, bistandsavtaler og informasjonsutvekslingsavtaler (TIEAS), avhengig av hvilket land det skal innhentes opplysninger fra.[133]

Erfaringer med innhenting:

Riksprosjekt E-handel har blant annet sendt bistandsanmodning til Luxembourg for å få kontoopplysninger for kunder av en betalingstjenestetilbyder, etter først å ha forsøkt å få opplysningene fra skattepliktig. De mottok opplysningene de ba om, men erfaringen er at anmodningen må være veldig konkret og nøyaktig på hva som etterspørres for å unngå å motta ustrukturert informasjon som kan være vanskelig å ta i bruk.

Kontrollmiljøene erfarer at selv om tilbyderen av betalingstjenesten har opprettet et datterselskap i Norge, vil informasjon om kundenes transaksjoner allikevel være eiet av morselskapet i utlandet, og dermed være utilgjengelig for skattemyndighetene uten bruk av bistandsanmodning.

Utvikling

I fagmiljøene innen e-handel i Skatteetaten, er oppfatningen at antall saker hvor nyere betalingstjenester er benyttet øker. For Skatteetaten er spørsmålet hvorvidt eier av nettbutikken oppgir omsetningen til beskatning i Norge.

Det er videre en oppfatning at nyere betalingstjenester i stor grad har tatt over fra konvensjonelle "banktjenester" etter innføringen av betalingsformidlingsforbudet i 2010. Det er en mulighet for at Skatteetatens satsning på området har medført at en

[133] Tax Information Exchange Agreements. Bistandsavtaler med 41 tidligere lukkede jurisdiksjoner. For informasjon om skatteavtaler, inkl. TIEAS, se www.regjeringen.no Skatteavtaler mellom Norge og andre stater

del spillere har gått over til mindre synlige betalingskanaler for mottak eller bruk av gevinster opptjent i utlandet, eksempelvis kort tilknyttet netellerkonto eller lignende e-wallets.

Samarbeid

Internett-sentrene i de nordiske landenes skattemyndigheter møtes årlig i regi av Nordisk Agenda, hvor også tidligere teknisk senter i Riksprosjekt E-handel har deltatt. Her er som regel nyere betalingsløsninger et av flere tema på agendaen. Sist høst hadde IOTA en egen workshop om pengespor i e-handel, hvor riksprosjektet deltok. Formålet for samarbeidet er kunnskaps- og erfaringsdeling.

Politiet

Øko-teamene har mye erfaring med bruk av ulike forhåndsbetalte kort i saker de etterforsker. Kortene lades opp med utbytte fra ulike former for vinningskriminalitet, blant annet grove bedragerier, underslag og salg av narkotika.

Kripos har etterforsket saker på "det mørke nettet" hvor betalingen for narkotika har skjedd med kryptovaluta, hvorpå utbyttet i stor grad har blitt tatt ut med forhåndsbetalte kort som er registrert ved bruk av falske identiteter. De falske identitetene er kjøpt på "det mørke nettet".

Politiet oppgir å ha lite eller ingen erfaringer med saker hvor mobile betalingstjenester er benyttet.

Det er gjort desto fler erfaringer med saker hvor det er benyttet internettbaserte betalingstjenester. Politiet har observert at utbytte fra ulike former for vinningskriminalitet, samt trygdebedragerier, har vært overført til utenlandske spillselskaper gjennom en rekke forskjellige internettbaserte betalingstjenester. I tillegg ser politiet at betaling for live streaming av overgrep mot barn på internett skjer gjennom denne type betalingstjenester.

Politiet har flere erfaringer med betalinger i virtuell valuta. Svært ofte gjelder dette handel med narkotika, men det meldes også om én sak der det ble handlet bitcoins med utbyttet fra et bedrageri, hvorpå disse ble benyttet på nettspill. Kripos har sett tilfeller av at kryptovaluta benyttes som betalingsmiddel for ulike straffbare handlinger.

Innhenting av opplysninger

Ved innhenting av opplysninger fra norske aktører benyttes påleggskompetansen i straffeprosessloven § 210. Ovenfor kryptovalutavekslere har politiet fått utlevert opplysninger ved ordinære anmodninger om dette.

Ved innhenting av opplysninger fra aktører i utlandet er det praksis å sende henvendelse på forhånd om hva tjenesten krever for utlevering av informasjon. Alt fra anmodning fra politiet til ordinære rettsanmodninger benyttes.

Erfaringer med innhenting:

Øko-teamene opplyser om til dels lite erfaringer med å innhente opplysninger fra tilbydere av betalingstjenester. Det kreves ofte innhenting av informasjon fra utlandet og flere opplever å ha manglende kunnskap om hvordan, hvor og hvilken informasjon som kan innhentes.

Kripos melder om varierende erfaringer med å innhente opplysninger fra utenlandske tilbydere av betalingstjenester. I de tilfellene tjenesten kun har krevd en anmodning fra politiet og kontakten har vært direkte, er erfaringen at svar kommer raskt, og med mulighet til å etterspørre eventuell manglende informasjon. Ved rettsanmodninger tar det erfaringsmessig lang tid før svar kommer. Kvaliteten på informasjonen som utleveres er svært varierende, alt fra meget bra til dårlig eller ingen informasjon (informasjonen hevdes tapt av tjenesten).

ØKOKRIM v/ avdeling 3 beskriver en svært god erfaring med innhenting av opplysninger fra utenlandsk betalingstjenestetilbyder ved bruk av rettsanmodning. Lokalt politi tok henvendelsen videre og ba tilbyderen om de etterspurte opplysningene. ØKOKRIM mottok lister over alle transaksjonene betalingstjenestetilbyder hadde på siktede. Kvaliteten på opplysningene og responsen fra tilbyderen var svært god.

I øko-teamene er det en oppfatning av at oppklaringsprosenten på saker der nyere betalingstjenester er benyttet relativt sett er lav, da det er vanskelig å finne ut hvor pengene kommer fra, eller at nyere betalingstjenester i det hele tatt er benyttet. Noen gir tilbakemelding på at de av kapasitetshensyn ikke kan prioritere å forfølge denne type pengespor når primærlovbruddet først er avdekket og tilstrekkelig bevist. Hos ØKOKRIM derimot er oppfatningen at det skal være fullt mulig å kartlegge pengestrømmene, selv om det kan kreve noe mer ressurser.

Begrensninger

Kapasitet og kunnskap synes å være en tydelig begrensning i innhentingsprosessen i saker hvor nyere betalingstjenester er benyttet. Flere viser til arbeidsomfanget ved bruk av rettsanmodninger til utlandet, samt hvor lang tid det tar å få svar på anmodningen. Kripos har flere ganger opplevd at tjenesten som det skal innhentes informasjon fra har "mistet" data. Dette skyldes gjerne at tjenesten har blitt kjøpt opp eller blitt utsatt for dataangrep.

Utvikling

Noen av øko-teamene opplever en klar økning i antall saker hvor nyere betalingstjenester er benyttet, mens andre har enten ikke sett en økning, eller mener de har for lite grunnlag til å uttale seg om dette. Kripos melder imidlertid om en økning i saker som gjelder det “mørke nettet” og bruk av kryptovaluta.

Flere av teamene er av den oppfatning at sakene hvor nyere betalingstjenester er benyttet, er økende i kompleksitet og omfang. Det er merarbeid knyttet til innhenting fra utlandet, informasjon må hentes inn og sammenstilles fra flere kilder, og informasjonsmengden i sakene er større enn i andre saker. Videre er det utstrakt bruk av falske profiler og identiteter i sakene som ytterligere begrenser sporbarheten. Utfordringer med å få oversikt over pengestrømmene ved bruk av tradisjonelle og tilgjengelige etterforskingsmetoder bidrar til at sakene anses å være komplekse.

Samarbeid

Generelt vises det til gode erfaringer med tverretatlige samarbeid i saker der flere etater og tilsyn er involvert. Det synes imidlertid ikke å finnes samarbeidsfora der kunnskap om nyere betalingstjenester på et overordnet nivå naturlig kan utveksles. Unntaket her er Kripos v/ IRES som har hatt noe kunnskapsutveksling med Skatteetatens riksprosjekt på e-handel, vedrørende blant annet kryptovaluta og det

"mørke nettet". Kripos har også vært i kontakt med Senter for internettgranskning og digital utvikling (SIDU) i Skatteetaten, med tanke på et mer omfattende samarbeid. Formålet med et slikt samarbeid vil være å dele kunnskap om informasjonsinnhenting i åpne kilder (OSINT).

ØKOKRIM v/EFE samarbeider med tilsvarende enheter (FIU) i andre land gjennom "Egmont Group of Financial Intelligence Units" (Egmont). Gjennom dette samarbeidet utveksles etterretningsinformasjon innenfor området hvitvasking og terrorfinansiering. Landene er forpliktet til automatisk å utveksle informasjon dersom det identifiseres en knytning til det andre landet, og informasjonen anses som potensielt viktig for landet. EFE observerer at de gjennom dette samarbeidet fra tid til annen mottar informasjon vedrørende internettbaserte betalingsplattformer og forhåndsbetalte kort.

Felles problem, ulike utfordringer

Innhentet materiale viser at bruk av nyere betalingstjenester representerer et problem på tvers av etatene. Noen av tangeringspunktene er:

- Arbeidstilsynet, NAV Kontroll og Skatteetaten ser bruk av forhåndsbetalte kort som verktøy for å skjule lønnsutbetalinger.
- NAV Kontroll og Skatteetaten har observert ulike internettbaserte betalingstjenester benyttet slik at etatenes mulighet til å kartlegge aktivitet i nettbutikker utfordres.
- NAV Kontroll, Skatteetaten og politiet ser at internettbaserte betalingstjenester benyttes i forbindelse med nettspill hos utenlandske spillselskap.
- Tolletaten og politiet ser bruk av en rekke ulike nyere betalingstjenester i forbindelse med handel med ulovlige varer.

Det er en generell oppfatning at antall saker hvor nyere betalingstjenester er benyttet øker, samt at de er økende i kompleksitet og omfang.

Det er videre noen utfordringer knyttet til bruk av nyere betalingstjenester som flere av etatene synes å ha til felles. Disse er:

- Fragmentert kompetanse på området
- Lite kunnskap om betalingstjenestetilbydere
- Utfordringer knyttet til innhenting av opplysninger fra utlandet

Det er bred enighet om at generell kompetanseheving vil føre til økt bevissthet blant kontrollørene slik at flere pengestrømmer gjennom nyere betalingstjenester avdekkes. Økt kunnskap vil medføre mer effektiv forfølgelse av pengespor og fremskaffelse av dokumentasjon. Det er videre uttrykt ønske om at økt kunnskap kan gi større muligheter for sikring og inndragning av verdier (gjelder spesielt politiet og Skatteetaten).

Hva gjelder innhenting av opplysninger fra utlandet, er grad av- og bakgrunnen for utfordringene forskjellig fra etat til etat:

- Arbeidstilsynet anser ikke bruk av nyere betalingstjenester å være særlig relevant for deres arbeid, og har derfor ikke utfordringer knyttet til innhenting fra utlandet.

- Tolletaten innhenter hovedsakelig ikke opplysninger fra tilbydere, men mottar opplysninger fra importørene frivillig med bakgrunn i plikter som følger av tolloven. Innhenting fra utlandet er derfor ikke relevant. Økt bruk av nyere betalingstjenester representerer imidlertid en utfordring for tolletatens etterretningsarbeid knyttet til kjøp av ulovlige varer.
- I NAV kontroll begrenses kontrollarbeidet av at de ikke har hjemler til å innhente opplysninger fra utenlandske tjenestetilbydere.
- Skatteetaten gir uttrykk for at de opplever å ha gode hjemler og prosesser for innhenting fra utlandet. Noen miljøer viser til nyttige erfaringer om hvordan anmodninger bør utformes for å gi best mulig resultat. Det er imidlertid ofte utfordrende å finne frem til hvem som har de nødvendige opplysningene. I noen tilfeller uteblir også svar fra betalingstjenestetilbyderen.
- For politiets del synes manglende kapasitet og kunnskap om innhenting fra tjenestetilbyder i utlandet å være en tydelig begrensning. Det er videre stor variasjon i erfaringene med bruk av rettsanmodninger til utlandet. Noen miljøer opplever at innhenting gjennom rettsanmodninger er svært tidkrevende, og ofte resultatløst. Særorganene deler ikke oppfatningen av at bruk av rettsanmodninger er særskilt utfordrende.

Kriterier for at etatene skal kunne møte de utfordringene som bruk av nyere betalingstjenester representerer, er:

- Dedikerte, oppdaterte kompetansemiljøer øker kunnskapen i å avdekke, forfølge og dokumentere spor av transaksjoner ved bruk av nyere betalingstjenester.
- Gode rutiner og prosesser ved anmodninger til utlandet gjør opplysninger som betalingstjenestetilbyder innehar mer tilgjengelig, og effektiviserer innhentingen.
- Deling av kunnskap, erfaringer og metodebruk - internt i- og på tvers av etatene.

En vurdering av trusselen nyere betalingstjenester utgjør mot etatenes arbeid med bekjempelse av økonomisk kriminalitet følger av trusselvurderingen.

Vedlegg 1 Begrepsforklaringer

Fintech er en forkortelse for Financial technology.[134] Teknologiselskaper, både startups og etablerte teknologiselskaper benytter teknologi for å tilby eksisterende finansielle tjenester til lavere kostnader samt gode tekniske løsninger.

Det andre bankdirektivet stadfester at en finansinstitusjon etablert i en EU-stat fritt kan etablere og drive tilsvarende virksomhet i andre EU-stater.[135] En finansinstitusjon skal kun trenge en tillatelse for å drive virksomhet i alle medlemslandene.

Ved grensekryssende virksomhet tilbys tjenester direkte fra hovedkontoret i hjemlandet eller via en representant i vertslandet. Finansinstitusjonen eller forsikringsselskapet som ønsker å utøve grensekryssende virksomhet skal underrette tilsynsmyndigheten i hjemlandet om hvilke typer virksomheter den har til hensikt å utøve.

Aktører knyttet til betalingskort
Følgende er aktører er involvert i systemet rundt betalingskort, inkludert forhåndsbetalte kort:[136]

Kortutsteder – Den som utsteder kortene og som kundene har en fordring på ved innskudd på de forhåndsbetalte kortene. Banker og finansinstitusjoner kan utstede kort. Eksempel på dette er Sparebank1 SMN som utsteder Spendon forhåndsbetalte kort.

Innløser – De som utfører transaksjonen fra kunden til forhandler og er den som godkjenner at forhandler kan tilby bruk av kort overfor kundene. Et eksempel på en innløser er Teller.[137]

Erverver – Den som legger opp infrastrukturen for å kunne godta kortbetaling, ha en relasjon med forhandleren og opererer kontoen der inntektene fra en handel blir satt inn. De som legger opp betalingsinfrastrukturen er bankene selv, eksempelvis DNB.

Distributør– Den som distribuerer de forhåndsbetalte kortene til salgsleddet. Eksempel på en distributør er Paygoo som distribuerer kort utgitt av Wirecard Card Solutions.

Betalingsnettverksoperatør – Den som står for den tekniske plattformen for å kunne gjennomføre en transaksjon, eksempelvis Visa og Mastercard.

Agent – Den som tilbyr forhåndsbetalte korttjenester på vegne av andre som utsteder kort. Eksempelvis kan Rema 1000 være agent for Spendon.

Betalingsgateway - Leverandør av nettsiden der kunden kan legge inn kortopplysningene.[138] Gatewayen står også for kommunikasjon mellom innløser og hjemmesiden til forhandler. Eksempel på en gateway er epay.[139]

---

[134] www.pwc.com What is fintech
[135] eur-lex.europa.eu 89/646/EØF
[136] FATF Guidance for a risk based approach Prepaid cards, Mobile payments and internet-based payment services, 2013 (Side 6)
[137] www.nets.eu "bestill avtale"
[138] Blog.epay.no – Hva er forskjellen på en betalingsgateway og en innløser?

Ny forordning om opplysninger som skal følge en betaling i betalingskjeden. Sammen med det 4. hvitvaskingsdirektiv ble det fremmet forslag om ny forordning (EU) nr. 847/2015 som skal avløse forordning (EF) nr. 1781/2006.

Formålet med forordningen er å forhindre at finanssektoren misbrukes av kriminelle til å hvitvaske penger og å finansiere terrorisme. Forordningen gir regler om hvilken informasjon om betaler og betalingsmottaker som skal følge pengeoverføringer gjennom betalingskjeden. Dette gjør det mulig å spore betalinger i større grad enn i dag, siden forordningen som avløses ikke stiller krav om at informasjon om betalingsmottaker skal følge betalinger.[140]

[139] http://tech.epay.dk/nn/faq-introduction
[140] NOU 2016:27 Kapittel 11.

Vedlegg 2 Regelverk

Betalingstjenestedirektiv nr. 1 (PSD – Payment Service Directive)

Betalingstjenestedirektivet nr. 1 fra 2007 gir et rettslig grunnlag for et felles marked i EU området for betalinger.[141] Direktivet skal også legge grunnlaget for at betalinger blir sikrere og at tjenestene blir mer innovative over hele EU på samme måte som internt i det enkelte EU-land. Følgene av dette er blant annet at det har blitt et større utvalg av tjenester og større konkurranse i betalingsmarkedet, lavere gebyrer på overføringer og at overføringer tar kortere tid. I tillegg har markedet for overføring på tvers av landegrensene i EU blitt større og transaksjonene blitt raskere.[142] Direktivet var en del av arbeidet med å få fri flyt av varer, personer, kapital og tjenester i EU. Betalingsdirektivet medførte samordnede regler om tilsyn, tilgang på markedet for nye betalingstjenester, opplysningskrav, rettigheter og forpliktelser for tilbydere og brukere av betalingstjenestene.

E-penger

Direktivet begrenser utstedelse av e-penger, det er kun finansinstitusjoner som har adgang til utstedelse av e-penger. Betalingsforetak har ikke mulighet til å utstede e-penger etter betalingstjenestedirektivet.[143] For tilbydere som ikke utsteder e-penger eller tar imot innskudd blir det i direktivet innført et nytt begrep "betalingsinstitusjoner". Disse betalingsinstitusjonene må ha krav om tilsyn, forsvarlig kapital og krav til utarbeidelse av årsregnskap.[144] Foretak som oppfyller nasjonale vilkår kan yte grensekryssende virksomhet og etablere virksomhet i andre EU-stater samt yte begrenset kreditt i inntil ett år.[145]

Tjenesteyters plikter

Betalingstjenestedirektivet fastsetter tjenesteyterens opplysningsplikt. Videre fastsetter direktivet regler om hvordan informasjon skal gis betaleren og betalingsmottakeren, samt regler om autorisasjon av betalingsoppdrag, utførelse av betalingsoppdrag, maksimal tid for gjennomføring av betalingsoppdrag, renteberegning ved betalingsoverføringer, tjenesteyterens ansvar for transaksjonen og midlene, tjenestetilbyders og betalers ansvar for tap ved uautoriserte betalingstransaksjoner, og om sanksjoner og utenomrettslige klageordninger.

Unntak

Enkelte betalingstjenester er unntatt fra konsesjonsplikt slik som teleoperatører i tilfeller der de ikke opptrer som mellomledd, eksempelvis innhold som kun kan benyttes på mobiltelefonen. Også betalingstjenester i et begrenset nettverk er unntatt, eksempelvis betalingsinstrument som bare kan benyttes til kjøp av varer og tjenester fra én forretning eller et begrenset nettverk av forretninger.

---

[141] Europa.eu – Direktiv 2007/64/EF – Om betalingstjenester i det indre marked og om endring av direktiv 97/7/EF, 2002/65/EF, 2005/60/EF og 2006/48/EF og om opphevelse av direktiv 97/5/EF på dansk.

[142] europa.eu Payment services directive: frequently asked questions

[143] Jf. finansavtaleloven § 1 andre ledd bokstav g). (?)

[144] europa.eu Payment services directive: frequently asked questions

[145] www.europalov.no Betalingstjenestedirektivet

Betalingstjenestedirektivet i norsk lov
PSD ble i 2010 gjennomført i norsk lov i finansforetaksloven, finansavtaleloven og betalingssystemloven.

Betalingstjenestedirektiv nr. 2 (PSD2-Payment service directive 2)

PSD2 har som overordnet formål å beskytte kundene og få billigere, sikre og moderne betalingstjenester. Forordningene om interbankgebyr og SEPA forordningen skal også være med på å sikre dette.[146] Ved å legge til rette for innovasjon og tilgang til nye aktører fremmes konkurranse, særlig betalingstjenester innen mobil og internett. Det meste av PSD er videreført i PSD2, slik som regulering av tilbydere av betalingstjenester, herunder e-pengeforetak, betalingstjenesteforetak og kredittinstitusjoner.

Andre tjenestetilbyderes tilgang til bankkonto
I forbindelse med at bankene må legge til rette for å gi betalingstjenestetilbydere tilgang til konto er det kommet to nye typer tjenester på markedet: betalingsinitieringstjeneste og betalingstjenestetilbydere. Disse blir regulert i det nye direktivet.

Betalingsinitieringstjenester vil kunne tilbys av betalingstjenestetilbyderen betalingsfullmektiger og vil være et alternativ til å betale med kort.[147] Tjenesten vil kunne initiere en betaling på vegne av kunden,men vil vanligvis ikke råde over pengene ved en transaksjon. Allerede går 55 prosent av internettbetalinger gjennom denne typen tjenester i Nederland. Eksempel på slike tjenester som eksisterer i dag i Europa er Sofort Banking og Trustly.[148]

Kontoopplysningstjenester vil kunne tilbys av betalingstjenestetilbyderen opplysningsfullmektiger og kan gi en total oversikt over bankkontoer hos forskjellige betalingstjenestetilbydere. Informasjonen som kontoinformasjonstjenestene får tilgang til, kan brukes til å vise kunden hva de har brukt penger på og hjelpe til med budsjettering og finansiell planlegging. Eksempler på slike tjenester i dag er Mint og Moven.[149]

Betalingstjenestetilbydere, deriblant betalingsinitieringstjenester, vil kunne tilby kort tilknyttet bankkonto i bank som de ikke kontrollerer, og gjennomføre betalinger på bakgrunn av dette.[150]

---

[146] Finanstilsynet: Utkast til høringsnotat, innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. www.regjeringen.no (Side 5)
[147] Finanstilsynet: Utkast til høringsnotat, innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. www.regjeringen.no (Side 5)
[148] www.accenture.com Accenture banking opportunities EU PSD2
[149] www.accenture.com Accenture banking opportunities EU PSD2
[150] Finanstilsynet: Utkast til høringsnotat, innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. www.regjeringen.no (Side 6)

Forbrukerbeskyttelse
Forbrukerbeskyttelsen styrkes i direktivet som følge av betalingstjenestenes mulighet for tilgang til konto, blant annet gjennom sterk autentisiering fra kundene og krav til sikkerhet i kommunikasjonen mellom betalingstjenestetilbyderne. PSD2 begrenser videre størrelsen på transaksjonsgebyr for debet/kredittkort og ved debiteringer i Euro og kredittoverførsler.[151]

Unntak
Nytt for dette direktivet vedrørende begrensede nettverk er at tjenester basert på betalingsinstrumenter som bare er gyldige i én medlemsstat på forespørsel fra et foretak eller offentlig myndighet, trenger ikke konsesjon. De må ha sosiale- eller skatteformål og være regulert av myndighetene. Videre skal de kun brukes til kjøp av spesifikke varer eller tjenester fra leverandører som har inngått avtale med utstederen av betalingsinstrumentet.[152]

Direktivet medfører utvidelse av unntak i forhold til dagens norske regulering når det gjelder *teleoperatører*. Direktivet fastslår at billettkjøp og kjøp av digitalt innhold som faktureres med telefonregning skal unntas.Imidlertid vil det være en begrensning på 50 Euro per transaksjon og 300 Euro per måned.

Rettslig vurdering av elektroniske penger (E-penger)

Et alternativ til kontanter er elektroniske penger. Betaling kan skje elektronisk fra et kort, mobiltelefon eller over internett.[153]

Den Europeiske sentralbanken (ECB) definerer e-penger til å være:

> *"elektronisk lagret pengeverdi på en teknisk enhet som kan bli brukt til å utføre betaling overfor andre enn dem som utsteder e-penger. Enheten fungerer som et instrument for å bære forhåndsbetalte penger uten nødvendigvis involvere bankkontoer i transaksjonene. E-pengeproduktene kan være maskinvarebasert eller programvarebasert, avhengig av hvilken teknologi som brukes for å lagre pengeverdien."*[154] [155]

Norsk lovgivning om e-penger
I henhold til finansforetaksloven er elektroniske penger (E-penger) "elektronisk lagret pengeverdi representert ved en fordring på utstederen, som er utstedt etter mottak av

[151] Finanstilsynet: Utkast til høringsnotat, innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. www.regjeringen.no (Side 6)
[152] Finanstilsynet: Utkast til høringsnotat, innføring av det reviderte betalingstjenestedirektivet (PSD2) I norsk rett. www.regjeringen.no (Side 12-13)
[153] Ec.europa.eu Overview
[154] Maskinvarebasert: Kjøpekraften ligger i en personlig fysisk enhet, eksempelvis et forhåndsbetalt kort med maskinvarebaserte sikkerhetsfunksjoner. Pengeverdier overføres vanligvis ved hjelp av lesere som ikke trenger sanntids nettverkstilkobling til en ekstern server.
[155] Programvarebasert: Programvarebaserte produkter bruker spesialprogramvare som fungerer på vanlige personlige enheter som datamaskiner eller tablets(Mobiltelefoner). For å muliggjøre en overføring av pengeverdi må enheten være tilkoblet internett mot en ekstern server som styrer bruken av kjøpekraft. Det eksisterer også kombinasjoner av maskinvarebaserte og programvarebaserte produkter.

midler for å utføre betalingstransaksjoner, og som er anerkjent som betalingsmiddel av andre enn utstederen." [156]

En elektronisk lagret pengeverdi som benyttes til å gjennomføre betalingstransaksjoner som bare kan benyttes til å kjøpe varer eller tjenester hos en leverandør innenfor et begrenset nettverk av leverandører, regnes ikke som elektroniske penger.

I Norge er det bare banker, kredittforetak, e-pengeforetak og finansieringsforetak som har lov til å utstede elektroniske penger.[157] Likevel kan utenlandske kredittinstitusjoner og e-pengeforetak utstede e-penger i Norge.

Krav på innløsning av e-pengefordringen foreldes i utgangspunktet ikke, men det skal være en avtale mellom utstederen og ihendehaveren der vilkårene rundt innløsning fremkommer. Utstederen av elektroniske penger skal, når ihendehaveren krever det, kunne innløse de elektroniske pengene. [158]

Foretak som har konsesjon som e-pengeforetak gis adgang til å utstede elektroniske penger og å utføre betalingstjenester og motta betalingsmidler fra kunder til bruk ved utførelsen av tjenestene.[159]

E-pengeforetak har ikke adgang til å ta renter av elektroniske penger. E-pengeforetak skal, uten ugrunnet opphold, omgjøre betalingsmidler til penger.[160]

E-pengedirektivene
EU-direktivene skal i EU-området samkjøre kravene for e-penge-tjenester og gi felles krav til e-pengeforetak.[161] Dessuten skal direktivet sørge for at nykommere skal få tilgang til markedet dersom de oppfyller visse vilkår. Nærmere om EUs e-pengedirektiver følger:

<u>E-penge-direktivet 2000/46/EF</u>
Det er og har vært en rask utvikling innen elektronisk handel og formålet med dette direktivet var å sette rammer, som gjør at fordelene ved elektroniske penger kan benyttes og utvikles. Tilbydere av elektroniske penger gis et begrenset virksomhetsområde, og medlemsstatenes lover og forskrifter, og hvordan det skal føres tilsyn med dem, må samordnes på tvers av medlemsstatene.

Det fastslås at direktivet betrakter elektroniske penger som erstatning for mynter og sedler. Det sørges for at institusjoner som utsteder e-penger kommer under tilsyn, at elektroniske penger må kunne innløses etter pålydende verdi og at institusjonene har tilstrekkelig egenkapital (1 million Euro). Tilsynsordninger bør være målrettet og enklere enn for andre kredittinstitusjoner, men samtidig bør det være bestemmelser som er strengere enn for andre kredittinstitusjoner i forhold til hva de kan utøve.

<u>E-penge direktivet 2009/110/EF</u>

[156] Lov 10. april 2015 nr 17 om finansforetak og finanskonsern, finansforetakslovens § 2-4
[157] Finansforetakslovens § 2-4
[158] Finansforetakslovens § 13-20
[159] Finansforetakslovens § 2-11
[160] Finansforetakslovens § 13-19
[161] Europa.eu – e-money – "Overview"

Direktivet avløste direktiv 2000/46/EF. EU-parlamentet mente det var flere hindre for det åpne markedet for elektroniske pengetjenester.[162] Direktivet sørger for å fjerne hindre for tilbydere samt tilpasses betalingstjenestedirektivet 2007/64/EF.[163]

Direktivet er begrenset til betalingstjenesteytere som utsteder e-penger. Direktivet omfatter ikke tilbydere av forhåndsbetalte betalingsinstrumenter (forhåndsbetalte betalingskort) som tilbys for betaling i én butikk, eller kjede- eller kundekort, (bensinkort, medlemskort, reisekort, matkuponger eller tjenestekuponger). Disse kommer bare under direktivets virkeområde dersom de utvikler seg fra å gjelde særskilte formål til generelle formål. Direktivet kommer heller ikke til anvendelse ved kjøp av digitale varer eller tjenester som kun tilfører varen eller tjenesten en egenverdi, eksempelvis en ringetone til en mobiltelefon.

Tidligere var det ikke mulig for e-pengeforetak å gjøre noe annet enn å utstede e-penger. Dette blir nå utvidet med dette direktivet, noe som særlig gjelder telekommunikasjonsselskap. Startkapital for e-pengeforetak settes ned fra 1 million Euro til 350 000 Euro. Sist, men ikke minst, ble det fastsatt krav til forbrukerbeskyttelse.

E-pengeforetak bør ifølge direktivet ikke kunne utstedes av agenter bortsett fra betalingstjenester nevnt i direktiv 2007/64/EF.

Utstedelse av e-penger regnes ikke som innskudd og bør benyttes til betaling av beløp som vanligvis er begrensede og ikke bli brukt til sparing. De kan ikke lånes ut.

[162] europa.eu – official journal of the europeean union
[163] Regjeringen.no – om e-pengedirektivet

Finanstilsynets rolle

Finanstilsynet er et selvstendig styringsorgan som bygger på lover og vedtak fra Stortinget, regjeringen og Finansdepartementet og på internasjonale standarder for finansielt tilsyn.[164] Finanstilsynet skal bidra til finansiell stabilitet gjennom tilsyn og sørge for at brukerne kan stole på at finansielle avtaler og tjenester blir fulgt opp. De samarbeider med andre lands tilsynsmyndigheter rundt regelverksutvikling.

Finanstilsynets virksomhet
Finanstilsynet skal blant annet føre tilsyn med banker, kredittforetak, finansieringsforetak, betalingsforetak og e-pengeforetak. Dette gjelder også tilsvarende utenlandske foretak som driver virksomhet i Norge.[165]

Finanstilsynet skal se til at de foretak de har tilsyn med virker på en hensiktsmessig og betryggende måte og se til at de ivaretar forbrukernes rettigheter og interesser.[166] Finanstilsynet skal granske regnskaper og andre oppgaver fra foretakene og ellers gjøre de undersøkelser Finanstilsynet finner nødvendig. Foretaket plikter å legge frem blant annet foretakets protokoller, registrerte regnskapsopplysninger, regnskapsmateriale, bøker, dokumenter, datamaskiner eller annet teknisk hjelpemiddel. Videre plikter revisor å rapportere til Finanstilsynet forhold som de får kjennskap til gjennom revisjon. Dette kan være overtredelser, forhold som medfører at regnskapet ikke blir godkjent, og forhold som kan skade videre drift.

Finanstilsynet kan etter § 4 i finanstilsynsloven pålegge foretak under tilsyn blant annet å innrette revisjon etter regler fastsatt av tilsynet, innrette internkontrollen etter tilsynets bestemmelser, sende oppgaver og opplysninger som tilsynet bestemmer, ha en høyere egenkapital enn minstekapital og ha en lavere kreditt overfor kunder enn høyeste grense.

Videre kan Finanstilsynet pålegge stans av virksomhet når tilsynet finner at virksomheten driver uten nødvendig tillatelse.[167]

Finansforetak skal rapportere til Finanstilsynet forhold som er nødvendige for å vurdere risikoen knyttet til virksomheten. [168] [169] Dette gjelder blant annet ansvarlig kapital, kapitalkrav og andre nødvendige forhold.

Finanstilsynet skal se til at banker, kredittforetak, finansieringsforetak, og holdingforetak i finanskonsern med slike foretak, har klare retningslinjer og rutiner for overvåking, vurdering, styring og kontroll av risiko og kapitalrisiko.[170]
Finanstilsynet skal sikre betryggende soliditet, risikobevissthet og styring og kontroll i foretakene. Tilsynsvirksomheten består av stedlig og dokumentbasert tilsyn.

---

[164] www.finanstilsynet.no Om finanstilsynet
[165] Lov 7. desember 1956 nr. 1 om tilsyn med finansforetak mv. Finanstilsynsloven § 1
[166] Finanstilsynsloven § 3
[167] Finanstilsynsloven § 4a
[168] Finansforetaksloven § 1–3 – Finansforetak som driver virksomhet som bank, kredittforetak, finansieringsforetak, forsikringsforetak, pensjonsforetak og holdingforetak i finanskonsern. Også betalingsforetak eller e-pengeforetak som er gitt tillatelse for å drive denne typen virksomhet.
[169] Lov 10. april 2015 nr. 17 om finansforetak og finanskonsern. Finansforetaksloven § 13–8
[170] Finansforetaksloven § 14–6

Konsesjon fra Finanstilsynet
Finanstilsynet krever at (blant annet) banker, kredittforetak, finansieringsforetak, betalingsforetak, e-pengeforetak samt grensekryssende foretak må ha konsesjon for å kunne drive i Norge.

Finanstilsynsloven gir oversikt over hva de forskjellige konsesjonene gir av tillatelser:

Bank: Konsesjon som bank gir mulighet til å ta imot innskudd, yte kreditt, stille garanti for egen regning og til å yte betalingstjenester.[171] I tillegg kan banken drive annen finansieringsvirksomhet, utstedelse av e-penger, forretninger for foretakets eller kundens regning i penge-, valuta- og verdipapirmarkedet samt andre banktjenester.[172]

Kredittforetak: Med konsesjon som kredittforetak kan virksomheten motta andre betalingspliktige midler enn innskudd, yte kreditt og stille garantier for egen regning. I tillegg kan det inkludere annen finansieringsvirksomhet, forretninger for foretakets regning i penger, fremmed valuta og verdipapirmarkedet, utstedelse av e-penger, ytelse av betalingstjenester eller andre særlige tjenester.[173]

Finansieringsforetak: Konsesjon som finansieringsforetak gir adgang til blant annet å drive med leasing, factoring og annen finansieringsvirksomhet, forretninger for foretakets eller kunders regning i penge- eller valutamarkedet, omsetning av valuta eller andre særlige tjenester. I tillegg kan det gis tillatelse til å drive virksomhet som e-pengeforetak eller som betalingsforetak, men kan ikke ta i mot tilbakebetalingspliktige midler fra allmennheten.[174]

Betalingsforetak: Konsesjon som betalingsforetak gir adgang til å motta betalingsmidler fra kunder til bruk for å utføre betalingstjenester. Betalingsforetak kan også få tillatelse til å drive som finansieringsforetak. Finanstilsynet kan gi begrenset tillatelse til å yte betalingstjenester kun i Norge til foretak med hovedkontor og forretningskontor i Norge eller filial av foretak fra annen EØS-stat med begrenset tillatelse derfra.[175]

E-pengeforetak: Konsesjon som e-pengeforetak gir adgang til å utstede elektroniske penger, utføre betalingstjenester og til å motta betalingsmidler fra kunder.[176] E-pengeforetak kan også gis tillatelse til å drive som finansieringsforetak.[177]

Søknad om konsesjon sendes til Finanstilsynet mens departementet gir tillatelsene.[178]

---

[171] Lov 10. april 2015 nr 17 om finansforetak og finanskonsern, Finansforetaksloven § 2-3 - Betalingstjenester kan bare utføres av banker, kredittforetak, betalingsforetak, e-pengeforetak og finansieringsforetak. Utenlandske kredittinstitusjoner, betalingsforetak og e-pengeforetak har også rett til å utføre betalingstjenester i Norge. I tillegg kommer også omsetning av valuta i forbindelse med penge overføring til utlandet.
[172] Finansforetaksloven § 2–7
[173] Finansforetaksloven § 2–8
[174] Finansforetaksloven § 2–9
[175] Finansforetaksloven § 2–10
[176] Finansforetaksloven § 2–4 – Elektroniske penger kan bare utstedes av banker, kredittforetak, e-pengeforetak og av finansieringsforetak som kan drive virksomhet i Norge samt av utenlandske kredittinstitusjoner og e-pengeforetak med adgang til å drive i landet. De elektroniske pengene kan benyttes til å utføre betalingstransaksjoner.
[177] Finansforetaksloven § 2-11

Hos Finanstilsynet er det per 4.4.2017 registrert 15 betalingsforetak, seks e-pengeforetak, 39 filialer av utenlandsk kredittinstitusjon (NUF), 126 banker og 34 kredittforetak. I tillegg var det registrert 336 grensekryssende betalingsforetak, 15 betalingsforetak som hadde meldt om agenter, 93 grensekryssende e-pengeforetak og 388 kredittinstitusjoner.

Utenlandske finansforetaks virksomhet i Norge

Finansforetaksloven kapittel 5 angår utenlandske finansforetaks virksomhet her i landet. Datterforetak av utenlandsk finansinstitusjon og filial av utenlandsk foretak i annen EØS-stat, kan gis konsesjon til å drive virksomhet i Norge. Ved grensekryssende virksomhet kan tillatelse gis for finansinstitusjon, forsikringsforetak, pensjonsforetak, betalingsforetak og e-pengeforetak med hovedsete i en annen EØS-stat, så lenge foretaket har tillatelse og er under tilsyn fra myndighetene i hjemstaten.[179] En måned etter at Finanstilsynet har mottatt nødvendige opplysninger fra hjemstatens tilsynsmyndigheter kan foretaket starte sin grensekryssende virksomhet i Norge.

Det stilles krav etter finansforetaksloven. Blant annet gjelder dette at et finansforetak skal organiseres og drives på en forsvarlig måte, dessuten ha en klar organisasjonsstruktur og ansvarsfordeling. I tillegg skal foretaket vurdere risiko, enkeltvis og samlet, blant annet hvilken systemrisiko virksomheten har, samt ha tilstrekkelig likvide eiendeler for å dekke sine forpliktelser ved forfall.[180]

[178] Lov 10. april 2015 nr 17 om finansforetak og finanskonsern, Finansforetaksloven § 3-1 og § 3-2
[179] Finansforetaksloven § 5-5
[180] Finansforetaksloven § 13-5 - 13-7

Hvitvaskingsregelverket

Generelt
Hvitvaskingsloven (hvvl.) har som formål å forebygge og avdekke transaksjoner med tilknytning til utbytte av straffbare handlinger eller med tilknytning til terrorhandlinger, jf. hvvl. § 1.[181]

Rapporteringspliktige etter hvitvaskingsloven er banker, kredittforetak og finansieringsforetak, e-pengeforetak, foretak som driver valutavirksomhet, betalingsforetak og andre som har rett til å yte betalingstjenester, med flere. Disse følger av hvvl. § 4.

Kundekontroll
Rapporteringspliktige skal foreta kundekontroll etter hvvl. §§ 6 til 13 og løpende oppfølging etter § 14. Kundekontroll og løpende oppfølging skal foretas på grunnlag av en vurdering av risiko for transaksjoner med tilknytning til utbytte av straffbare handlinger eller forhold som rammes av straffeloven §§ 131 til 136 a, der risikoen vurderes ut fra type kunde, kundeforhold, produkt eller transaksjon, jf. hvvl. § 5.[182]

Rapporteringspliktige skal foreta kundekontroll ved

1. etablering av kundeforhold,

2. transaksjon som gjelder 100 000 kroner eller mer, for kunde som den rapporteringspliktige ikke har et etablert kundeforhold til,

3. mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller forhold som rammes av straffeloven §§ 131 til 136 a, eller

4. tvil om hvorvidt tidligere innhentede opplysninger om kunden er korrekte eller tilstrekkelige.[183]

[181] Lov 6. mars 2009 nr. 11 om tiltak mot hvitvasking og terrorfinansiering mv.
[182] Prinsippet om risikobasert kundekontroll er grunnleggende i hvitvaskingsregelverket, bygger på "kjenn-din-kunde-prinsippet". Se lovkommentar i Gyldendal Rettsdata til hvvl. § 5.
[183] Hvvl. § 6.

Kundekontroll skal omfatte

1. registrering av opplysninger som nevnt i § 8,

2. bekreftelse av kundens identitet på grunnlag av gyldig legitimasjon,

3. bekreftelse av identiteten til reelle rettighetshavere på grunnlag av egnede tiltak, og

4. innhenting av opplysninger om kundeforholdets formål og tilsiktede art.[184]

Unntak fra plikt til å foreta normal kundekontroll følger av hvitvaskings*forskriften* § 10.[185] Unntaket gjelder plikten til å foreta kundekontroll etter hvitvaskingsloven § 6 første ledd nr. 1, 2 og 4, som gjengitt over.[186]

Slik forenklet kundekontroll kan gjennomføres blant annet ved utstedelse av elektroniske penger, når

i) det høyeste beløp som lagres på det elektroniske mediet er 250 Euro og mediet ikke kan lades opp igjen, eller

ii) det fastsettes en grense på 2 500 Euro for det samlede overførte beløp i et kalenderår, med mindre ihendehaveren har innløst et beløp på minst 1 000 Euro i samme kalenderår.[187] [188]

Følgende opplysninger skal uansett registreres ved opprettelse av konto i henhold til hvvl. § 13 andre ledd:

i) fullt navn eller foretaksnavn

ii) fødsels- eller organisasjonsnummer

iii) kundens faste adresse[189]

Finanstilsynet anbefaler at samme informasjon også registreres der det ikke blir etablert konto, og vilkårene for å foreta forenklet kundekontroll er tilstede.[190]

Tersklene for krav til identifikasjon og legitimasjon ved utstedelse av elektroniske penger følger således av hvitvaskingsforskriften § 10. Ved beløp på mer enn 250 Euro må brukeren gi opplysninger ved opprettelse av konto, og det er krav om legitimasjon. Er beløpet *lavere* enn 250 Euro, står rapporteringspliktige fritt, og kan unnta fra kundekontroll (dvs. la brukeren være anonym).

---

[184] Hvvl. § 7.
[185] jf. hvvl. § 13
[186] Merk at unntaket ikke gjelder for nr. 3 - ved mistanke om at en transaksjon har tilknytning til utbytte av straffbar handling eller forhold som rammes av straffeloven §§ 131 til 136 a
[187] Tidligere beløpsgrense 150 Euro. Endret 24.8.2010.
[188] Det vil si at man kan overføre inntil 2 500 Euro via det elektroniske mediet i løpet av et kalenderår, med mindre det gjøres et uttak på 1 000 Euro eller mer i det samme kalenderåret.
[189] Gitt ved hvvl. § 8 første til tredje ledd.
[190] Finanstilsynets rundskriv 24/2016 Kapittel 3.

EU-kommisjonen la 5. juli 2016 frem forslag om endringer i 4. hvitvaskingsdirektiv, som blant annet innebærer endringer knyttet til forhåndsbetalte instrumenter. Kommisjonen ønsker å redusere bruken av anonyme forhåndsbetalte betalingskort, ved å redusere grensen for krav til identifikasjon fra 250 til 150 Euro, samtidig som kravene til kundekontroll utvides. Videre inngår i forslaget at forhåndsbetalte kort utstedt utenfor EU bare skal kunne brukes i EU når disse oppfyller krav som svarer til 4. hvitvaskingsdirektiv.[191]

Rapporteringsplikt
Har rapporteringspliktige mistanke om at en transaksjon har tilknytning til utbytte av en straffbar handling, skal det foretas nærmere undersøkelser for å få bekreftet eller avkreftet mistanken. Dersom undersøkelsene ikke avkrefter mistanken, skal den rapporteringspliktige av eget tiltak oversende opplysninger til ØKOKRIM om den aktuelle transaksjonen og om de forhold som har medført mistanke.[192]

Ny hvitvaskingslov - Virtuell valuta
I NOU 2016:27 ble en ny hvitvaskingslov - som svarer til EUs 4. hvitvaskingsdirektiv og ny EU-forordning om informasjon som skal følge betalinger - foreslått. Utvalget vurderte blant annet om det bør innføres rapporteringsplikt etter hvitvaskingsloven for foretak som veksler virtuell valuta. Utvalget anså den manglende reguleringen av virtuell valuta for å skape muligheter for utnyttelse til kriminelle formål. Utvalget konkluderte likevel med at det er problematisk å underlegge denne type virksomhet hvitvaskingsregelverket på nåværende tidspunkt. Utvalget begrunnet dette med at utvekslingsplattformer ikke er regulert, og at dette fortsatt er en forholdsvis ny type virksomhet. Utvalget foreslo istedet forskriftshjemmel slik at anvendelsesområdet til hvitvaskingsloven kan utvides på et senere tidspunkt til å inkludere vekslingsplattformer for virtuell valuta.

I EU-kommisjonenes forslag til endringer i 4. hvitvaskingsdirektiv, foreslås imidlertid at tilbydere av vekslingstjenester mellom virtuelle penger og fysiske penger, samt såkalte wallet providers skal omfattes av direktivet.[193] Dette innebærer i tilfelle at tilbydere av vekslingstjenester må følge direktivets krav om å gjennomføre forebyggende tiltak og rapportere mistenkelige transaksjoner.

Europaparlamentet og Rådet er pr. mai 2017 fortsatt i forhandlinger om revidert hvitvaskingsdirektiv.

[191] Økonominytt fra EU-delegasjonen, Nr. 2 – Februar 2017.
[192] Hvvl. §§ 17 og 18.
[193] Wallet providers er leverandører av digitale lommebøker som gir tilgang til virtuelle penger

Rapporteringsplikt til valutaregisteret

Generelt
Valutaregisterets formål er å forebygge og bekjempe kriminalitet og bidra til riktig skatte- og avgiftsbetaling, ved at kontroll- og etterforskingsorganene får tilgang til opplysninger om valutavekslinger og fysisk eller elektronisk overføringer av betalingsmidler inn og ut av Norge.[194] Skattedirektoratet overtok 1.1.2016 behandlingsansvaret for registeret etter Toll- og avgiftsetaten.[195]

Det følger av valutaregisterloven § 6 at politiet, Skatteetaten, Tolletaten, Arbeids- og velferdsdirektoratet og Finanstilsynet skal ha tilgang til opplysningene i registeret. Søk i registeret skal kun skje ut fra etatenes behov for opplysninger i forbindelse med forebygging og bekjempelse av kriminalitet, kontrollvirksomhet og tilsyn.

Opplysninger i registeret slettes fem år etter utløpet av registreringsåret.[196]

Rapporteringsplikt
Etter valutaregisterloven § 4 skal foretak som kan drive valutavirksomhet, rapportere om valutaveksling og om overføring av betalingsmidler inn og ut av Norge.[197] [198] Toll- og avgiftsetaten skal rapportere om fysisk inn- og utførsel av valuta som overstiger NOK 25 000.

Rapporteringen skal inneholde opplysninger som identifiserer person eller foretak som mottar og sender, eller fører betalingsmidler inn eller ut av Norge, samt opplysninger om transaksjonen og betalingsmiddelet, jf. valutaregisterloven § 5. Beløpsgrenser og hvilke opplysninger som skal følge med de ulike typene overføringer følger av valutaregister*forskriften* §§ 9-13.

[194] Lov 28. mai 2004 nr. 29 om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge (valutaregisterloven) § 1.
[195] Ref. Valutaregisterforskriften § 1
[196] jf. Valutaregisterloven § 7
[197] Banker, betalingsforetak, e-pengeforetak og finansieringsforetak som har tillatelse til å drive valutavirksomhet, jf. Finansforetaksloven § 2-5 (1)
[198] Som valutavirksomhet regnes virksomhet som består i omsetning av valuta, jf. Finansforetaksloven § 2-5 (2)

Hvilke vekslinger og overføringer som konkret innrapporteres er:

- Betalingsformidling via bank
- Fysisk inn-/utførsel av betalingsmidler over NOK 25 000
- Bruk av norske kort i utlandet
    - Enkelttransaksjoner over NOK 25 000
    - Sum pr. kort/land/måned for beløp lavere eller lik NOK 25 000
- Bruk av utenlandske kort i Norge
    - Enkelttransaksjoner over NOK 25 000
    - Sum pr. kort pr. måned for beløp lavere eller lik NOK 25 000
    - Sum pr. brukersted pr. måned for beløp lavere eller lik NOK 25 000
    - Kontantuttak av beløp over NOK 5 000
- Transportørtransaksjoner (andre som overfører penger for eksempel Moneygram og Western Union)
- Valutaveksling, rapporteringspliktiges kjøp/salg av valuta i Norge over NOK 5 000

For betalingstjenestene som rapporten omhandler innebærer dette følgende:

- Bruk av forhåndsbetalte kort som innebærer grensekryssende transaksjoner rapporteres til valutaregisteret på lik linje med andre betalingskort.
- Ved bruk av internettbaserte betalingstjenester vil overføringer av penger mellom Norge og utlandet bli rapportert til valutaregisteret av banken som tilbyderen benytter. Hvorvidt innrapporteringen til valutaregisteret inneholder informasjon om den som ønsker overføringen gjennomført, varierer. Det samme gjelder for mobile betalingstjenester, i den grad de lar seg benytte til grensekryssende transaksjoner.
- Transaksjoner ved virtuell valuta fremgår ikke av valutaregisteret, da den ikke er ansett som en valuta av norske myndigheter. Grensekryssende betalinger ved norske parters kjøp eller salg av virtuell valuta hos aktører i utlandet, vil imidlertid fremkomme.

På oppdrag fra Finansdepartementet er det satt i gang et lovarbeid i Skattedirektoratet som blant annet berører hvem som skal ha tilgang til valutaregisteret, og hvordan tilgang til opplysninger i registeret skal reguleres. Skattedirektoratet skal også vurdere om ordlyden i valutaregisterloven § 4 bør endres for å fange opp aktører som faller utenfor regelverket, men som bør være omfattet av rapporteringsplikten.[199]

[199] Ref. oppdragsbrev fra Finansdepartementet av 16. februar 2017, Del 1, punkt 2

Utveksling av finansielle kontoopplysninger etter FATCA og CRS

Norge har, som ett av 100 land, forpliktet seg til gjensidig automatisk utveksling av finansielle kontoopplysninger etter OECDs nye internasjonale standard, kjent som "the Common Reporting Standard" (CRS).[200] Standarden bygger på en modellavtale for automatisk informasjonsutveksling som Norge - i likhet med en rekke andre land - har inngått med USA. Avtalen med USA er kjent som "Foreign Account Tax Compliance Act" (FATCA).

Norske tredjeparters rapporteringsplikt for finansielle forhold følger av skatteforvaltningsloven § 7-3, hvor avtalenes forpliktelser er innarbeidet.[201] Tredjeparten skal identifisere hvor kontohaver og eventuelle reelle rettighetshavere tilknyttet den finansielle kontoen er skattemessig hjemmehørende, og informasjon om denne skal utveksles med det respektive utland.[202] Utvekslingen skjer årlig via skattemyndighetene.[203]

Blant annet banker, kredittforetak, finansieringsforetak og e-pengeforetak har plikt til å gi opplysninger om kundens finansielle forhold. Det skal blant annet gis opplysninger om innskuddskontoer.[204]

Mottak av betalingsmidler for å utstede elektroniske penger regnes ikke som innskudd.[205] Det samme gjelder for betalingsmidler mottatt av betalingsforetak eller e-pengeforetak ved oppdrag om betalingstjenester[206]. Likevel vil "innskudd" i e-penger kunne omfattes av opplysningsplikten i og med at e-pengeforetak er omfattet.[207]

Den opplysningspliktige skal gi opplysninger om *produktet* ("innskuddet" i e-penger i denne sammenheng) og om *subjekter* som er knyttet til produktet (det vil si eier av e-pengene - kontohaver). Reglene knyttet til identifisering av kontohaver hviler på bestemmelsene om kundekontroll i hvitvaskingsregelverket, herunder også unntakene som tillater forenklet kundekontroll, som følger av hvitvaskingsforskriften § 10.

Dette innebærer at e-pengeforetak - og andre som utsteder e-penger - vil være rapporteringspliktige for kundenes "innskudd" i e-penger, men bare i de tilfeller hvor

---

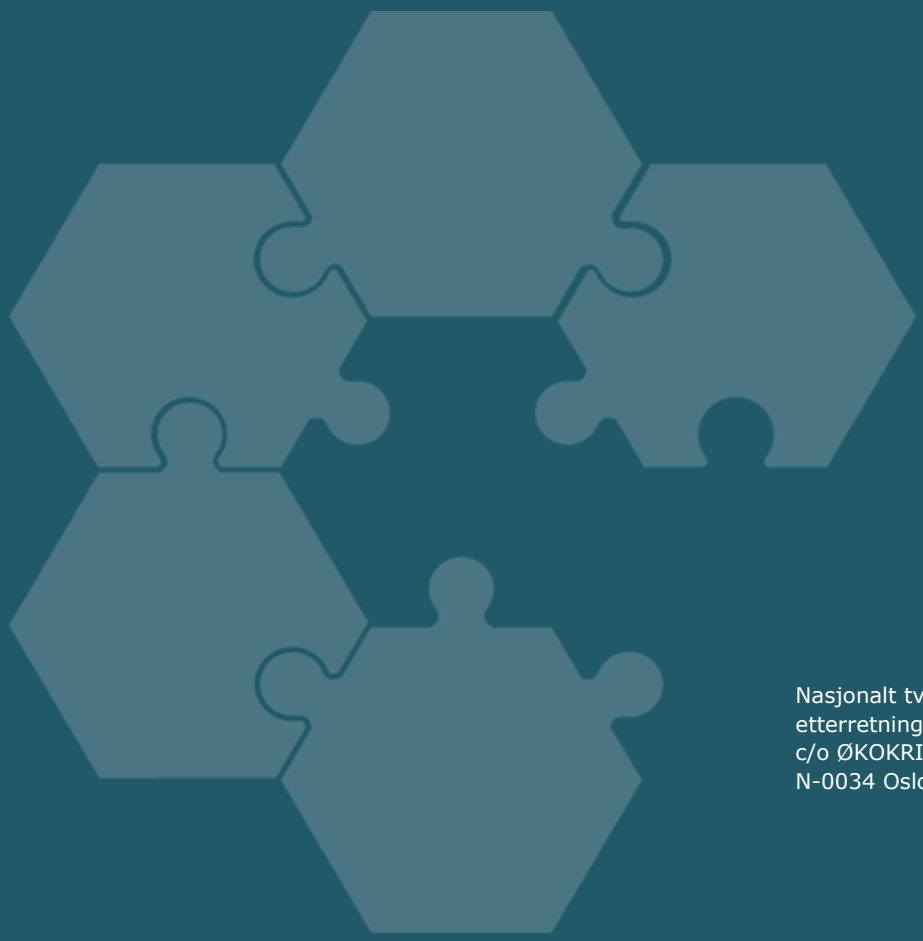
[200] Oversikt over hvilke land som har inngått CRS-avtale fremgår av https://www.oecd.org CRS by jurisdiction
[201] Lov 27. mai 2016 nr. 14 om skatteforvaltning.
[202] Hva som regnes som finansielle konti fremgår av samleforskrift om tredjeparters opplysningsplikt av 17. september 2013 nr. 1092 § 5-3-32.
[203] Den første utvekslingen av opplysninger mellom USA og Norge etter FATCA fant sted i september 2015. Første utveksling av opplysninger etter CRS vil skje i september 2017.
[204] Skatteforvaltningsloven § 7-3.
[205] Finansforetaksloven § 2-2 andre ledd.
[206] Hva som regnes som betalingstjenester følger av finansavtaleloven § 11.
[207] Dette følger av forarbeidene til skatteforvaltningsloven § 7-3 (tidligere ligningsloven § 5-3): *"Det ble i høringsnotatet lagt til grunn at e-pengeforetak vil kunne falle inn under samlebestemmelsen i høringsnotatets lovforslag § 5-3 nr. 1 bokstav j., og at "innskudd" i e-penger dermed vil kunne omfattes av opplysningsplikten. Skattedirektoratet har i sin høringsuttalelse uttalt at e-pengeforetak bør nevnes særskilt i opplistingen, slik at det klargjøres at slike foretak omfattes av opplysningsplikten. Departementet har etter en ny vurdering kommet til at det er hensiktsmessig at e-pengeforetak tas inn særskilt i lovteksten.",* Prop. 1LS (2015-2016), punkt 18.5.2, *"Hvem som er opplysningspliktige"*

innskuddet er høyere enn 250 Euro, eller det ikke er fastsatt en grense på 2 500 Euro for det samlede overførte beløp i et kalenderår[208] - gitt at ikke andre vilkår for forenklet kundekontroll er til stede.[209]

Betalingsforetak er ikke omfattet av opplysningsplikten.

Pr. april 2017 er det kun seks foretak som har konsesjon som e-pengeforetak i Norge, jf. Finanstilsynets konsesjonsregister. Samtidig er det 93 e-pengeforetak som har meldt om grensekryssende virksomhet til Norge.[210] Dersom norske skattemyndigheter gjennom FATCA og CRS i fremtiden mottar opplysninger om nordmenns beholdninger av e-penger fra over 100 land, vil dette kunne bidra til å redusere risiko knyttet til betalingstjenester hvor e-penger benyttes.

[208] "... med mindre ihendehaveren har innløst et beløp på minst 1 000 Euro i samme kalenderår."
[209] OECD har ikke publisert en fortolkning av spørsmålet om innskudd i e-penger er omfattet av rapporteringsplikten etter CRS, det kan derfor være forskjellig praksis i de ulike land som har inngått avtalen.
[210] Liste over virksomheter som har meldt grensekryssende virksomhet til Norge fins på Finanstilsynets hjemmesider



Nasjonalt tverretatlig analyse- og etterretningssenter
c/o ØKOKRIM, Postboks 8193, dep,
N-0034 Oslo