DELEGERT KOMMISJONSFORORDNING (EU) 2018/389 **2023/EØS/34/17**

av 27. november 2017

om utfylling av europaparlaments- og rådsdirektiv (EU) 2015/2366 med hensyn til tekniske reguleringsstandarder for sterk kundeautentisering og felles og sikre åpne kommunikasjonsstandarder(*)

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF([1]), særlig artikkel 98 nr. 4 annet ledd, og

ut fra følgende betraktninger:

1) Betalingstjenester som tilbys elektronisk, bør utføres på en sikker måte og benytte teknologi som kan garantere sikker autentisering av brukeren og i størst mulig grad redusere risikoen for bedrageri. Autentiseringsprosedyren bør generelt omfatte transaksjonsovervåkingsordninger som kan avsløre forsøk på å gjøre bruk av en betalingstjenestebrukers tapte, stjålne eller urettmessig tilegnede personaliserte sikkerhetsopplysninger, og bør også sikre at betalingstjenestebrukeren er den rettmessige brukeren og derfor gir sitt samtykke til overføring av midler og tilgang til sine kontoopplysninger ved normal bruk av de personaliserte sikkerhetsopplysningene. Det er videre nødvendig å spesifisere kravene om sterk kundeautentisering som bør stilles hver gang en betaler får nettbasert tilgang til sin betalingskonto, initierer en elektronisk betalingstransaksjon eller utfører en handling via en fjernkanal, noe som kan innebære risiko for betalingsbedrageri eller andre former for misbruk, ved å kreve generering av en autentiseringskode som bør være motstandsdyktig mot forfalskning i sin helhet og mot visning av noen av elementene som koden ble generert fra.

2) Ettersom bedragerimetodene hele tiden er i endring, bør kravene om sterk kundeautentisering fremme innovative tekniske løsninger som håndterer framveksten av nye trusler mot sikre elektroniske betalinger. For å sikre at kravene som fastsettes, til enhver tid oppfylles på en effektiv måte, er det også rimelig å kreve at sikkerhetstiltakene for anvendelse av sterk kundeautentisering og unntakene fra dette, tiltakene for å beskytte de personaliserte sikkerhets-opplysningenes fortrolighet og integritet og tiltakene for å innføre felles og sikre åpne kommunikasjonsstandarder dokumenteres, testes regelmessig, evalueres og revideres av operasjonelt uavhengige revisorer med ekspertise innen IT-sikkerhet og betalinger. For å gi vedkommende myndigheter mulighet til å overvåke kvaliteten på gjennomgåelsen av disse tiltakene bør disse gjennomgåelsene gjøres tilgjengelige for dem på anmodning.

3) Siden elektroniske fjernbetalingstransaksjoner innebærer en høyere risiko for bedrageri, er det nødvendig å stille ytterligere krav om sterk kundeautentisering for slike transaksjoner for å sikre at elementene dynamisk knytter transaksjonen til et beløp og en betalingsmottaker som betaleren angir idet transaksjonen initieres.

4) Dynamisk tilknytning er mulig gjennom generering av autentiseringskoder som er underlagt et sett av strenge sikkerhetskrav. For å sikre teknologisk nøytralitet bør det ikke stilles krav om en bestemt teknologi for innføring av autentiseringskoder. Autentiseringskoder bør derfor bygge på løsninger som for eksempel generering og validering av engangspassord, digitale signaturer eller andre kryptografisk baserte valideringer med nøkler eller kryptografisk materiale lagret i autentiseringselementene, så lenge sikkerhetskravene oppfylles.

(*) Denne unionsrettsakten, kunngjort i EUT L 69 av 13.3.2018, s. 23, er omhandlet i EØS-komiteens beslutning nr. 159/2020 av 23. oktober 2020 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester), ennå ikke kunngjort.

([1]) EUT L 337 av 23.12.2015, s. 35.

5) Det er nødvendig å fastsette særlige krav for situasjoner der sluttbeløpet ikke er endelig kjent på tidspunktet da betaleren initierer en elektronisk fjernbetalingstransaksjon, for å sikre at den sterke kundeautentiseringen er spesifikk for maksimumsbeløpet som betaleren har gitt samtykke til, som omhandlet i direktiv (EU) 2015/2366.

6) For å sikre anvendelse av sterk kundeautentisering er det også nødvendig å kreve tilstrekkelige sikkerhetsegenskaper for elementene av sterk kundeautentisering som kategoriseres som «kunnskap» (noe bare brukeren kjenner til), for eksempel lengde eller kompleksitet, for elementene som kategoriseres som «besittelse» (noe bare brukeren har), for eksempel algoritmespesifikasjoner, nøkkellengde og informasjonsentropi, og for enhetene og programvaren som leser elementene som kategoriseres som «iboende egenskap» (noe brukeren er), for eksempel algoritmespesifikasjoner, biometrisk sensor og malbeskyttelse, særlig for å redusere risikoen for at disse elementene avdekkes av, formidles til og brukes av uautoriserte parter. Det er også nødvendig å fastsette krav som sikrer at disse elementene er uavhengige av hverandre, slik at brudd på ett av elementene ikke svekker de andre elementenes pålitelighet, særlig når disse elementene brukes via en flerfunksjonsenhet, for eksempel et nettbrett eller en mobiltelefon, som kan brukes både til å gi instruksjoner om å utføre betalingen og i autentiseringsprosessen.

7) Kravene om sterk kundeautentisering gjelder betalinger initiert av betaleren, uansett om betaleren er en fysisk person eller en juridisk person.

8) Det ligger i sakens natur at betalinger som foretas gjennom et anonymt betalingsinstrument, ikke er omfattet av kravet om sterk kundeautentisering. Dersom slike instrumenters anonymitet fjernes av avtalemessige eller lovgivningsmessige årsaker, skal betalingene omfattes av sikkerhetskravene som følger av direktiv (EU) 2015/2366 og denne tekniske reguleringsstandarden.

9) I samsvar med direktiv (EU) 2015/2366 fastsettes unntak fra prinsippet om sterk kundeautentisering basert på transaksjonens risikonivå, beløp og tilbakevendende karakter og på betalingskanalen som brukes ved gjennomføringen av betalingstransaksjonen.

10) Handlinger som innebærer tilgang til saldoen og de seneste transaksjonene på en betalingskonto uten å avsløre sensitiv betalingsinformasjon, gjentatte betalinger til samme betalingsmottakere, som tidligere er blitt opprettet eller bekreftet av betaleren ved hjelp av sterk kundeautentisering, og betalinger til og fra samme fysiske eller juridiske person som har kontoer hos samme betalingstjenesteyter, utgjør en begrenset risiko og gir derfor betalingstjenesteytere mulighet til ikke å anvende sterk kundeautentisering. Her ses det bort fra at i samsvar med artikkel 65, 66 og 67 i direktiv (EU) 2015/2366 bør ytere av betalingsinitieringstjenester, betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, og ytere av kontoopplysningstjenester bare anmode om og innhente de opplysningene fra kontotilbyderen som er nødvendige og vesentlige for å kunne levere en gitt betalingstjeneste med betalingstjenestebrukerens samtykke. Et slikt samtykke kan gis individuelt for hver anmodning om opplysninger eller for hver betaling som skal initieres, eller for ytere av kontoopplysningstjenester som et mandat for utpekte betalingskontoer og tilhørende betalingstransaksjoner som fastsatt i den kontraktsmessige avtalen med betalingstjenestebrukeren.

11) Unntak for små kontaktløse betalinger på utsalgssteder, der det også tas hensyn til et største antall påfølgende transaksjoner eller et bestemt fast maksimumsbeløp for påfølgende transaksjoner uten å anvende sterk kundeautentisering, gjør det mulig å utvikle brukervennlige betalingstjenester med lav risiko, og dette bør derfor tas i betraktning. Det bør også innføres unntak for elektroniske betalingstransaksjoner initiert gjennom ubetjente terminaler, der det av driftsmessige årsaker ikke alltid er så enkelt å gjennomføre bruk av sterk kundeautentisering (for eksempel for å unngå kø og mulige trafikkulykker ved bomstasjoner eller for å unngå andre sikkerhetsrisikoer).

12) I likhet med unntaket for små kontaktløse betalinger på utsalgssteder er det nødvendig å finne en passende balanse mellom ønsket om utvidet sikkerhet for fjernbetalinger og behovet for brukervennlige og tilgjengelige betalinger innenfor e-handel. I samsvar med disse prinsippene bør det fastsettes forsiktige terskelverdier under hvilke det ikke er nødvendig å anvende sterk kundeautentisering, slik at bare mindre kjøp på nettet omfattes. Større forsiktighet bør utvises ved fastsettelse av terskelverdier for kjøp på nettet for å ta hensyn til det faktum at personen ikke er fysisk til stede når kjøpet foretas, noe som utgjør en noe høyere sikkerhetsrisiko.

13) Kravene om sterk kundeautentisering gjelder betalinger initiert av betaleren, uansett om betaleren er en fysisk person eller en juridisk person. Mange foretaksbetalinger initieres gjennom særskilte prosesser eller protokoller som sørger for det høye sikkerhetsnivået for betalinger som direktiv (EU) 2015/2366 tar sikte på å oppnå gjennom sterk kundeautentisering. Dersom vedkommende myndigheter slår fast at disse betalingsprosessene og -protokollene, som bare gjøres tilgjengelige for betalere som ikke er forbrukere, oppfyller målene i direktiv (EU) 2015/2366 med hensyn til sikkerhet, kan betalingstjenesteytere, med hensyn til disse prosessene eller protokollene, unntas fra kravene om sterk kundeautentisering.

14) Ved transaksjonsrisikoanalyser i sanntid som kategoriserer en betalingstransaksjon som en transaksjon med lav risiko, bør det også innføres et unntak for betalingstjenesteytere som ikke har til hensikt å anvende sterk kundeautentisering, dersom det stilles effektive og risikobaserte krav som sikrer betalingstjenestebrukerens midler og personopplysninger. Disse risikobaserte kravene bør kombinere resultatene fra risikoanalysen, som bekrefter at det ikke er identifisert unormale utgifts- eller atferdsmønstre hos betaleren, og tar hensyn til andre risikofaktorer, herunder opplysninger om betalerens og betalingsmottakerens tilholdssted, med beløpsmessige terskelverdier basert på bedragerifrekvenser beregnet for fjernbetalinger. Dersom en betaling på grunnlag av transaksjonsrisikoanalyser i sanntid ikke kan kategoriseres som en transaksjon med lav risiko, bør betalingstjenesteyteren gå tilbake til sterk kundeautentisering. Det høyeste beløpet for slike risikobaserte unntak bør fastsettes på en måte som sikrer en svært lav tilhørende bedragerifrekvens, også sammenlignet med bedragerifrekvensen for alle betalingstjenesteyterens betalingstransaksjoner, herunder slike som autentiseres gjennom sterk kundeautentisering, innenfor et visst tidsrom og på løpende basis.

15) For å sikre en effektiv gjennomføring bør betalingstjenesteytere som ønsker å dra nytte av unntakene fra sterk kundeautentisering, for hver type betalingstransaksjon regelmessig overvåke og på anmodning tilgjengeliggjøre for vedkommende myndigheter og Den europeiske banktilsynsmyndighet (EBA) verdien av bedragerske eller uautoriserte betalingstransaksjoner og den observerte bedragerifrekvensen for alle egne betalingstransaksjoner, uansett om de er autentisert gjennom sterk kundeautentisering eller gjennomført i henhold til et relevant unntak.

16) Innsamlingen av disse nye historiske opplysningene om bedragerifrekvensen for elektroniske betalingstransaksjoner vil også være et bidrag til EBAs effektive gjennomgåelse av terskelverdiene for unntak fra sterk kundeautentisering basert på transaksjonsrisikoanalyse i sanntid. EBA bør gjennomgå og ved behov oversende utkast til oppdateringer av disse tekniske reguleringsstandardene til Kommisjonen i form av forslag til nye terskelverdier og tilhørende bedragerifrekvenser for å forbedre sikkerheten til elektroniske fjernbetalinger i samsvar med artikkel 98 nr. 5 i direktiv (EU) 2015/2366 og artikkel 10 i europaparlaments- og rådsforordning (EU) nr. 1093/2010([1]).

17) Betalingstjenesteytere som gjør bruk av noen av de fastsatte unntakene, bør alltid kunne velge å bruke sterk kundeautentisering på handlingene og betalingstransaksjonene omhandlet i disse bestemmelsene.

18) Tiltakene som beskytter fortroligheten og integriteten til personaliserte sikkerhetsopplysninger og til autentiseringsenheter og programvare, bør begrense risikoen knyttet til bedrageri i form av uautorisert og bedragersk bruk av betalingsinstrumenter og uautorisert tilgang til betalingskontoer. Det er derfor nødvendig å innføre krav om sikker opprettelse og levering av personaliserte sikkerhetsopplysninger og om deres forbindelse til betalingstjenestebrukeren, og å fastsette vilkår for fornyelse og deaktivering av disse sikkerhetsopplysningene.

19) For å sørge for effektiv og sikker kommunikasjon mellom de relevante aktørene med hensyn til kontoopplysningstjenester, betalingsinitieringstjenester og bekreftelse av tilgang til midler er det nødvendig å spesifisere kravene til felles og sikre åpne kommunikasjonsstandarder som alle relevante betalingstjenesteytere må overholde. Direktiv (EU) 2015/2366 gir ytere av kontoopplysningstjenester tilgang til og rett til å bruke betalingskontoopplysninger. Denne forordningen endrer derfor ikke reglene for tilgang til andre kontoer enn betalingskontoer.

([1]) Europaparlaments- og rådsforordning (EU) nr. 1093/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske banktilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/78/EF (EUT L 331 av 15.12.2010, s. 12).

20) Enhver kontotilbyder med betalingskontoer som er tilgjengelige over nett, bør tilby minst ett tilgangsgrensesnitt som muliggjør sikker kommunikasjon med ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter. Grensesnittet bør gjøre det mulig for ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, å identifisere seg overfor kontotilbyderen. Det bør også gjøre det mulig for ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester å bruke autentiseringsprosedyrene som kontotilbyderen stiller til rådighet for betalingstjenestebrukeren. For å sikre teknologi- og forretningsmodellnøytralitet bør kontotilbydere fritt kunne velge om de vil tilby et særskilt grensesnitt for kommunikasjonen med ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, eller, for denne kommunikasjonen, tillate bruk av grensesnittet for identifisering av og kommunikasjon med kontotilbydernes betalingstjenestebrukere.

21) For å gjøre det mulig for ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, å utvikle egne tekniske løsninger bør grensesnittets tekniske spesifikasjoner behørig dokumenteres og gjøres offentlig tilgjengelig. Kontotilbyderen bør dessuten stille en innretning til rådighet som gjør det mulig for betalingstjenesteytere å teste de tekniske løsningene minst seks måneder før anvendelsesdatoen for disse reguleringsstandardene eller, dersom lanseringen finner sted etter standardenes anvendelsesdato, før datoen da grensesnittet lanseres på markedet. For å sikre samvirkingsevne mellom ulike teknologiske kommunikasjonsløsninger bør grensesnittet bruke kommunikasjonsstandarder utviklet av internasjonale eller europeiske standardiseringsorganisasjoner.

22) Kvaliteten på tjenestene som leveres av ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester, er avhengig av at grensesnittene som er innført eller tilpasset av kontotilbyderne, fungerer som de skal. Det er derfor viktig at det dersom grensesnittene ikke er i samsvar med bestemmelsene fastsatt i disse standardene, treffes tiltak som sikrer kontinuerlig drift for brukerne av de nevnte tjenestene. Det er nasjonale vedkommende myndigheters ansvar å sikre at ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester ikke blokkeres eller hindres når de leverer sine tjenester.

23) Dersom tilgang til betalingskontoer tilbys gjennom et særskilt grensesnitt, er det nødvendig å kreve at særskilte grensesnitt har tilsvarende tilgjengelighets- og ytelsesnivå som grensesnittet som er tilgjengelig for betalingstjenestebrukere, for å sikre betalingstjenestebrukeres rett til å benytte seg av ytere av betalingsinitieringstjenester og av tjenester som gir tilgang til kontoopplysninger, som fastsatt i direktiv (EU) 2015/2366. Kontotilbydere bør også fastsette transparente sentrale ytelsesindikatorer og servicenivåmål for tilgjengeligheten og ytelsen til særskilte grensesnitt, og de må være minst like omfattende som dem fastsatt for grensesnittet brukt av deres betalingstjenestebrukere. Disse grensesnittene bør testes av betalingstjenesteytere som skal bruke dem, og de bør stresstestes og overvåkes av vedkommende myndigheter.

24) For å sikre at betalingstjenesteytere som bruker det særskilte grensesnittet, kan fortsette å levere sine tjenester ved problemer med tilgjengelighet eller utilstrekkelig ytelse, er det nødvendig å stille til rådighet, på strenge vilkår, en reserveordning som vil gi slike leverandører mulighet til å bruke grensesnittet som kontotilbyderen opprettholder for identifisering av og kommunikasjon med egne betalingstjenestebrukere. Visse kontotilbydere kan unntas fra kravet om å stille til rådighet en slik reserveordning gjennom sine kundegrensesnitt dersom deres vedkommende myndigheter fastsetter at de særskilte grensesnittene oppfyller de særlige vilkårene som sikrer uhindret konkurranse. Dersom de særskilte grensesnittene som er omfattet av unntaket, ikke overholder de pålagte vilkårene, skal de aktuelle unntakene tilbakekalles av de berørte vedkommende myndighetene.

25) For å gjøre det mulig for vedkommende myndigheter å føre tilsyn med og overvåke gjennomføringen og håndteringen av kommunikasjonsgrensesnittene på en effektiv måte bør kontotilbyderen gjøre et sammendrag av den relevante dokumentasjonen tilgjengelig på sitt nettsted og på anmodning gi vedkommende myndigheter dokumentasjonen om kriseløsningene. Kontotilbydere bør også gjøre statistikk over tilgjengelighet og ytelse for grensesnittet offentlig tilgjengelig.

26) For å ivareta dataenes fortrolighet og integritet er det nødvendig å sørge for sikre kommunikasjonssesjoner mellom kontotilbydere, ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som

utsteder kortbaserte betalingsinstrumenter. Særlig er det nødvendig å kreve at sikker kryptering anvendes mellom ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester, betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, og kontotilbydere når de utveksler opplysninger.

27) For å styrke brukernes tillit og sikre sterk kundeautentisering bør det tas hensyn til bruk av elektroniske identifikasjonsmidler og tillitstjenester som omhandlet i europaparlaments- og rådsforordning (EU) No 910/2014([1]), særlig med hensyn til meldte ordninger for elektronisk identifikasjon.

28) For å sikre avstemte anvendelsesdatoer bør denne forordningen anvendes fra samme dato som da medlemsstatene må sikre at sikkerhetstiltakene omhandlet i artikkel 65, 66, 67 og 97 i direktiv (EU) 2015/2366 får anvendelse.

29) Denne forordningen bygger på utkastet til tekniske reguleringsstandarder som Den europeiske banktilsynsmyndighet (EBA) har framlagt for Kommisjonen.

30) EBA har holdt åpne og gjennomsiktige offentlige høringer om utkastet til tekniske reguleringsstandarder som ligger til grunn for denne forordningen, analysert de mulige tilknyttede kostnadene og fordelene samt innhentet uttalelse fra interessentgruppen for bankvirksomhet opprettet i samsvar med artikkel 37 i forordning (EU) nr. 1093/2010.

VEDTATT DENNE FORORDNINGEN:

KAPITTEL I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål

Denne forordningen fastsetter kravene som betalingstjenesteytere skal oppfylle ved gjennomføring av sikkerhetstiltak som gjør det mulig for dem å

a) anvende framgangsmåten for sterk kundeautentisering i samsvar med artikkel 97 i direktiv (EU) 2015/2366,

b) unnlate å anvende sikkerhetskravene for sterk kundeautentisering på særlige og begrensede vilkår basert på betalingstransaksjonens risikonivå, beløp og tilbakevendende karakter og på betalingskanalen som brukes ved gjennomføringen av transaksjonen,

c) beskytte fortroligheten og integriteten til betalingstjenestebrukerens personaliserte sikkerhetsopplysninger,

d) innføre felles og sikre åpne standarder for kommunikasjon mellom kontotilbydere, ytere av betalingsinitieringstjenester, ytere av kontoopplysningstjenester, betalere, betalingsmottakere og andre betalingstjenesteytere i forbindelse med levering og bruk av betalingstjenester i henhold til avdeling IV i direktiv (EU) 2015/2366.

Artikkel 2

Generelle autentiseringskrav

1. Betalingstjenesteytere skal ha innført transaksjonsovervåkingsordninger som gjør det mulig for dem å oppdage uautoriserte eller bedragerske betalingstransaksjoner ved gjennomføringen av sikkerhetstiltakene omhandlet i artikkel 1 bokstav a) og b).

([1]) Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (EUT L 257 av 28.8.2014, s. 53).

Disse ordningene skal bygge på analysen av betalingstransaksjoner, idet det tas hensyn til elementer som er typiske for betalingstjenestebrukeren ved normal bruk av de personaliserte sikkerhetsopplysningene.

2. Betalingstjenesteytere skal sikre at transaksjonsovervåkingsordninger minst tar hensyn til hver av følgende risikobaserte faktorer:

a) Lister over misbrukte eller stjålne autentiseringselementer.

b) Beløpet for hver betalingstransaksjon.

c) Kjente bedragerisценarioer i forbindelse med yting av betalingstjenester.

d) Tegn på infeksjon fra ondsinnet programvare i autentiseringsprosedyrens sesjoner.

e) Dersom tilgangsenheten eller programvaren leveres av betalingstjenesteyteren, en logg over bruken av tilgangsenheten eller programvaren som leveres til betalingstjenesteyteren, og over unormal bruk av tilgangsenheten eller programvaren.

Artikkel 3

Gjennomgåelse av sikkerhetstiltakene

1. Gjennomføringen av sikkerhetstiltakene omhandlet i artikkel 1 skal dokumenteres, regelmessig testes, evalueres og revideres i samsvar med betalingstjenesteyterens gjeldende rettslige ramme av revisorer som har ekspertise innen IT-sikkerhet og betalinger og er operasjonelt uavhengige innenfor eller av betalingstjenesteyteren.

2. Perioden mellom revisjonene omhandlet i nummer 1 skal fastsettes idet det tas hensyn til relevant ramme for regnskapsføring og lovfestet revisjon som gjelder for betalingstjenesteyteren.

Betalingstjenesteytere som benytter unntaket omhandlet i artikkel 18, skal imidlertid være gjenstand for en revisjon av metodikken, modellen og rapporterte bedragerifrekvenser minst hvert år. Revisoren som gjennomfører denne revisjonen, skal ha ekspertise innen IT-sikkerhet og betalinger og være operasjonelt uavhengig innenfor eller av betalingstjenesteyteren. Det første året unntaket omhandlet i artikkel 18 benyttes, og minst hvert tredje år deretter, eller oftere på vedkommende myndighets anmodning, skal denne revisjonen foretas av en uavhengig og kvalifisert ekstern revisor.

3. Revisjonen skal resultere i en evaluering av og en rapport om hvorvidt betalingstjenesteyterens sikkerhetstiltak er i samsvar med kravene fastsatt i denne forordningen.

Hele rapporten skal gjøres tilgjengelig for vedkommende myndigheter på anmodning.

KAPITTEL II

SIKKERHETSTILTAK FOR ANVENDELSE AV STERK KUNDEAUTENTISERING

Artikkel 4

Autentiseringskode

1. Dersom betalingstjenesteytere anvender sterk kundeautentisering i samsvar med artikkel 97 nr. 1 i direktiv (EU) 2015/2366, skal autentiseringen bygge på to eller flere elementer som kategoriseres som kunnskap, besittelse og iboende egenskap, og den skal resultere i generering av en autentiseringskode.

Autentiseringskoden skal aksepteres bare én gang av betalingstjenesteyteren, idet betaleren bruker autentiseringskoden til å få nettbasert tilgang til sin betalingskonto for å initiere en elektronisk betalingstransaksjon eller gjennomføre en handling via en fjernkanal, noe som kan innebære risiko for betalingsbedrageri eller annet misbruk.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere treffe sikkerhetstiltak for å sikre at alle følgende krav oppfylles:

a) Ingen opplysninger om noen av elementene omhandlet i nr. 1 kan utledes fra autentiseringskoden som utleveres.

b) Det er ikke mulig å generere en ny autentiseringskode basert på kunnskap om en autentiseringskode som er generert tidligere.

c) Autentiseringskoden kan ikke forfalskes.

3. Betalingstjenesteytere skal sikre at autentiseringen gjennom generering av en autentiseringskode omfatter alle følgende tiltak:

a) Dersom autentiseringen for fjerntilgang, elektroniske fjernbetalinger og andre handlinger via en fjernkanal som kan innebære risiko for betalingsbedrageri eller annet misbruk, ikke har generert en autentiseringskode med henblikk på nr. 1, skal det ikke være mulig å identifisere hvilket av elementene i nevnte nummer som var feilaktig.

b) Antallet mislykkede autentiseringsforsøk på rad før handlingene omhandlet i artikkel 97 nr. 1 blir midlertidig eller permanent blokkert, skal ikke overstige fem innenfor et gitt tidsrom.

c) Kommunikasjonssesjonene beskyttes mot fangst av autentiseringsdata som overføres under autentiseringen, og mot uautoriserte parters manipulering i samsvar med kravene i kapittel V.

d) Den lengste tiden betaleren kan være inaktiv etter å ha blitt autentisert for nettbasert tilgang til betalingskontoen, skal ikke overstige fem minutter.

4. Dersom blokkeringen omhandlet i nr. 3 bokstav b) er midlertidig, skal dens varighet og antall nye forsøk fastsettes på grunnlag av kjennetegnene til tjenesten som ytes til betaleren, og på grunnlag av alle relevante tilhørende risikoer, idet det minst tas hensyn til faktorene omhandlet i artikkel 2 nr. 2.

Betaleren skal varsles før blokkeringen gjøres permanent.

Dersom blokkeringen er gjort permanent, skal det etableres en sikker framgangsmåte som gjør det mulig for betaleren å begynne å bruke de blokkerte elektroniske betalingsinstrumentene igjen.

Artikkel 5

Dynamiske koblinger

1. Dersom betalingstjenesteytere anvender sterk kundeautentisering i samsvar med artikkel 97 nr. 2 i direktiv 2015/2366, skal de, i tillegg til kravene i artikkel 4 i denne forordningen, treffe sikkerhetstiltak som oppfyller alle følgende krav:

a) Betaleren informeres om betalingstransaksjonsbeløpet og om betalingsmottakeren.

b) Autentiseringskoden som genereres, er spesifikk for betalingstransaksjonsbeløpet og betalingsmottakeren som betaleren godkjente da transaksjonen ble initiert.

c) Autentiseringskoden som ble akseptert av betalingstjenesteyteren, svarer til det opprinnelige spesifikke betalingstransaksjonsbeløpet og identiteten til betalingsmottakeren som betaleren godkjente.

d) Enhver endring av beløpet eller betalingsmottakeren fører til at den genererte autentiseringskoden blir gjort ugyldig.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere treffe sikkerhetstiltak som sikrer fortroligheten, ektheten og integriteten til følgende:

a) Transaksjonsbeløpet og betalingsmottakeren i alle faser av autentiseringen.

b) Opplysningene som vises for betaleren i alle faser av autentiseringen, herunder generering, overføring og bruk av autentiseringskoden.

3. Med hensyn til nr. 1 bokstav b) og dersom betalingstjenesteytere anvender sterk kundeautentisering i samsvar med artikkel 97 nr. 2 i direktiv (EU) 2015/2366, får følgende krav anvendelse på autentiseringskoden:

a) I forbindelse med en kortbasert betalingstransaksjon der betaleren har gitt sitt samtykke til det nøyaktige beløpet som skal reserveres i samsvar med artikkel 75 nr. 1 i nevnte direktiv, skal autentiseringskoden være spesifikk for det beløpet som betaleren har gitt sitt samtykke til å reservere, og som betaleren godkjente da transaksjonen ble initiert.

b) I forbindelse med betalingstransaksjoner der betaleren har gitt sitt samtykke til å gjennomføre en serie av elektroniske fjernbetalingstransaksjoner til én eller flere betalingsmottakere, skal autentiseringskoden være spesifikk for det samlede beløpet for serien av betalingstransaksjoner og for de spesifiserte betalingsmottakerne.

Artikkel 6

Krav til elementene som kategoriseres som kunnskap

1. Betalingstjenesteytere skal treffe tiltak for å redusere risikoen for at de elementene av sterk kundeautentisering som kategoriseres som kunnskap, avdekkes av eller formidles til uautoriserte parter.

2. Betalerens bruk av disse elementene skal være gjenstand for risikoreduserende tiltak for å forhindre at de formidles til uautoriserte parter.

Artikkel 7

Krav til elementene som kategoriseres som besittelse

1. Betalingstjenesteytere skal treffe tiltak for å redusere risikoen for at de elementene av sterk kundeautentisering som kategoriseres som besittelse, brukes av uautoriserte parter.

2. Betalerens bruk av disse elementene skal være gjenstand for tiltak som skal forhindre at elementene reproduseres.

Artikkel 8

Krav til enheter og programvare knyttet til elementene som kategoriseres som iboende egenskap

1. Betalingstjenesteytere skal treffe tiltak for å redusere risikoen for at autentiseringselementene som kategoriseres som iboende egenskap og leses av tilgangsenheter og programvare som stilles til rådighet for betaleren, avdekkes av uautoriserte parter. Betalingstjenesteytere skal minst sikre at det er veldig lite sannsynlig at disse tilgangsenhetene og denne programvaren autentiserer en uautorisert part som betaleren.

2. Betalerens bruk av disse elementene skal være gjenstand for tiltak som sikrer at disse enhetene og denne programvaren sikrer beskyttelse mot uautorisert bruk av elementene gjennom tilgang til enhetene og programvaren.

Artikkel 9

Elementenes uavhengighet

1. Betalingstjenesteytere skal sikre at bruken av elementene av sterk kundeautentisering som er omhandlet i artikkel 6, 7 og 8, er gjenstand for tiltak som, når det gjelder teknologi, algoritmer og parametrer, sikrer at brudd på ett av elementene ikke svekker de andre elementenes pålitelighet.

2. Betalingstjenesteytere skal treffe sikkerhetstiltak dersom noen av elementene av sterk kundeautentisering eller selve autentiseringskoden brukes via en flerfunksjonsenhet, for å redusere risikoen som ville oppstå dersom flerfunksjonsenheten ble misbrukt.

3. Ved anvendelse av nr. 2 skal de risikoreduserende tiltakene omfatte hver av følgende:

a) Bruk av atskilte, sikre gjennomføringsmiljøer via programvaren som er installert i flerfunksjonsenheten.

b) Ordninger for å sikre at programvaren eller enheten ikke er blitt endret av betaleren eller av en tredjepart.

c) Dersom det er gjort endringer, ordninger for å begrense konsekvensene av dem.

KAPITTEL III

UNNTAK FRA STERK KUNDEAUTENTISERING

Artikkel 10

Betalingskontoopplysninger

1. Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de oppfyller kravene fastsatt i artikkel 2 og i nr. 2 i denne artikkelen, dersom en betalingstjenestebruker bare har nettbasert tilgang til én av eller begge følgende poster uten å utlevere sensitiv betalingsinformasjon:

a) Saldoen på én eller flere utpekte betalingskontoer.

b) Betalingstransaksjoner gjennomført i løpet av de seneste 90 dagene fra én eller flere utpekte betalingskontoer.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere ikke unntas fra anvendelsen av sterk kundeautentisering dersom et av følgende vilkår er oppfylt:

a) Betalingstjenestebrukeren får for første gang nettbasert tilgang til opplysningene angitt i nr. 1.

b) Det er gått mer enn 90 dager siden forrige gang betalingstjenestebrukeren hadde nettbasert tilgang til opplysningene angitt i nr. 1 bokstav b) og det ble anvendt sterk kundeautentisering.

Artikkel 11

Kontaktløse betalinger på utsalgsstedet

Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de overholder kravene fastsatt i artikkel 2, dersom betaleren initierer en kontaktløs elektronisk betalingstransaksjon og følgende vilkår er oppfylt:

a) Beløpet for hver enkelt kontaktløse elektroniske betalingstransaksjon overstiger ikke 50 euro.

b) Det samlede beløpet for tidligere kontaktløse elektroniske betalingstransaksjoner som er initiert ved hjelp av et betalingsinstrument med kontaktløs funksjonalitet fra seneste dato for anvendelse av sterk kundeautentisering, overstiger ikke 150 euro.

c) Antallet påfølgende kontaktløse elektroniske betalingstransaksjoner som er initiert via et betalingsinstrument med kontaktløs funksjonalitet siden seneste anvendelse av sterk kundeautentisering, overstiger ikke fem.

Artikkel 12

Ubemannede terminaler for transport- og parkeringsavgifter

Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de overholder kravene fastsatt i artikkel 2, dersom betaleren initierer en elektronisk betalingstransaksjon på en ubemannet betalingsterminal for å betale en transport- eller parkeringsavgift.

Artikkel 13

Betrodde begunstigede

1. Betalingstjenesteytere skal anvende sterk kundeautentisering dersom en betaler oppretter eller endrer en liste over betrodde begunstigede gjennom betalerens kontotilbyder.

2. Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de overholder de generelle autentiseringskravene, dersom betaleren initierer en betalingstransaksjon og betalingsmottakeren er oppført på en liste over betrodde begunstigede som betaleren tidligere har opprettet.

Artikkel 14

Gjentatte transaksjoner

1. Betalingstjenesteytere skal anvende sterk kundeautentisering dersom en betaler oppretter, endrer eller første gang initierer en serie av gjentatte transaksjoner med samme beløp og til samme betalingsmottaker.

2. Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de overholder de generelle autentiseringskravene, ved initiering av alle påfølgende betalingstransaksjoner som inngår i serien av betalingstransaksjoner omhandlet i nr. 1.

Artikkel 15

Kreditoverføringer mellom kontoer som innehas av samme fysiske eller juridiske person

Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering, forutsatt at de overholder kravene fastsatt i artikkel 2, dersom betaleren initierer en kreditoverføring under omstendigheter der betaleren og betalingsmottakeren er samme fysiske eller juridiske person og begge betalingskontoene innehas av samme kontotilbyder.

Artikkel 16

Små transaksjoner

Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering dersom betaleren initierer en elektronisk fjernbetalingstransaksjon og følgende vilkår er oppfylt:

a) Beløpet for den elektroniske fjernbetalingstransaksjon overstiger ikke 30 euro, og

b) det samlede beløpet for tidligere elektroniske fjernbetalingstransaksjoner som er initiert av betaleren siden seneste anvendelse av sterk kundeautentisering, overstiger ikke 100 euro, eller

c) antallet tidligere elektroniske fjernbetalingstransaksjoner som er initiert av betaleren siden seneste anvendelse av sterk kundeautentisering, overstiger ikke fem påfølgende enkeltstående elektroniske fjernbetalingstransaksjoner.

Artikkel 17

Sikre prosesser og protokoller for foretaksbetalinger

Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering for juridiske personer som initierer elektroniske betalingstransaksjoner ved bruk av særskilte betalingsprosesser eller -protokoller som stilles til rådighet for betalere som ikke er forbrukere, dersom vedkommende myndigheter anser at disse prosessene eller protokollene minst sikrer et likeverdig sikkerhetsnivå som det som er fastsatt i direktiv (EU) 2015/2366.

Artikkel 18

Transaksjonsrisikoanalyse

1. Betalingstjenesteytere skal kunne unnlate å anvende sterk kundeautentisering dersom betaleren initierer en elektronisk fjernbetalingstransaksjon som betalingstjenesteyteren anser å utgjøre en lav risiko i henhold til transaksjonsovervåkingsordningene omhandlet i artikkel 2 og i nr. 2 bokstav c) i denne artikkelen.

2. En elektronisk betalingstransaksjon omhandlet i nr. 1 skal anses å utgjøre en lav risiko dersom alle følgende vilkår er oppfylt:

a) Bedragerifrekvensen for denne typen transaksjon, som innberettet av betalingstjenesteyteren og beregnet i samsvar med artikkel 19, er lik eller lavere enn referansebedragerifrekvensen angitt i tabellen i vedlegget for henholdsvis «elektroniske kortbaserte fjernbetalinger» og «elektroniske fjernkreditoverføringer».

b) Transaksjonsbeløpet overstiger ikke den relevante terskelverdien for unntak («exemption threshold value», ETV) angitt i tabellen i vedlegget.

c) Etter å ha utført en risikoanalyse i sanntid har betalingstjenesteytere ikke påvist noe av følgende:

   i) Unormale utgifts- eller atferdsmønstre hos betaleren.

   ii) Uvanlige opplysninger om betalerens tilgang til enhet/programvare.

   iii) Infeksjon fra ondsinnet programvare i noen av autentiseringsprosedyrens sesjoner.

   iv) Kjente bedrageriscenarioer i forbindelse med yting av betalingstjenester.

   v) Unormalt tilholdssted for betaleren.

   vi) Høyrisikotilholdssted for betalingsmottakeren.

3. Betalingstjenesteytere som har til hensikt å unnta elektroniske fjernbetalingstransaksjoner fra sterk kundeautentisering fordi de anses å utgjøre en lav risiko, skal minst ta hensyn til følgende risikobaserte faktorer:

a) Tidligere utgiftsmønstre hos den enkelte betalingstjenestebruker.

b) Betalingstransaksjonshistorikken til hver av betalingstjenesteyternes betalingstjenestebrukere.

c) Tilholdsstedet for betaleren og betalingsmottakeren på tidspunktet for betalingstransaksjonen dersom tilgangsenheten eller programvaren stilles til rådighet av betalingstjenesteyteren.

d) Påvisning av unormale betalingsmønstre hos betalingstjenestebrukeren sett i forhold til brukerens betalingstransaksjonshistorikk.

Betalingstjenesteyterens vurdering skal kombinere alle disse risikobaserte faktorene til en risikoverdi for hver enkelt transaksjon for å avgjøre om en bestemt betaling bør tillates uten sterk kundeautentisering.

Artikkel 19

Beregning av bedragerifrekvenser

1. For hver type transaksjon omhandlet i tabellen i vedlegget skal betalingstjenesteyteren sikre at de samlede bedragerifrekvensene som omfatter både betalingstransaksjoner autentisert gjennom sterk kundeautentisering og betalingstransaksjoner gjennomført i henhold til et av unntakene omhandlet i artikkel 13–18, ikke overstiger referansebedragerifrekvensen for samme type betalingstransaksjon angitt i tabellen i vedlegget.

Samlet bedragerifrekvens for hver type transaksjon skal beregnes som samlet verdi av uautoriserte eller bedragerske fjerntransaksjoner, uansett om midlene er inndrevet eller ikke, dividert med samlet verdi av alle fjerntransaksjoner for samme type transaksjon, uansett om de er autentisert ved bruk av sterk kundeautentisering eller gjennomført i henhold til et av unntakene omhandlet i artikkel 13–18 på løpende kvartalsbasis (90 dager).

2. Beregningen av bedragerifrekvensene og resultatverdiene skal vurderes av revisjonen omhandlet i artikkel 3 nr. 2, som skal sikre at de er fullstendige og nøyaktige.

3. Metodikken og alle modeller som betalingstjenesteytere bruker til å beregne bedragerifrekvenser, samt selve bedragerifrekvensen skal behørig dokumenteres og gjøres tilgjengelig i fullt omfang for vedkommende myndigheter og EBA, med forhåndsmelding til berørte vedkommende myndigheter på anmodning.

Artikkel 20

Opphør av unntak basert på transaksjonsrisikoanalyse

1. Betalingstjenesteytere som gjør bruk av unntaket omhandlet i artikkel 18, skal umiddelbart varsle vedkommende myndigheter dersom en av bedragerifrekvensene de overvåker, for en type betalingstransaksjon angitt i tabellen i vedlegget, overstiger gjeldende referansebedragerifrekvens, og skal framlegge for vedkommende myndigheter en beskrivelse av tiltakene de har til hensikt å treffe for å sikre at bedragerifrekvensen de overvåker, igjen er i samsvar med gjeldende referanse-bedragerifrekvenser.

2. Betalingstjenesteytere skal umiddelbart slutte å gjøre bruk av unntaket omhandlet i artikkel 18 for alle typer betalingstransaksjoner som er angitt i tabellen i vedlegget i det spesifikke terskelverdiintervallet for unntak, dersom bedragerifrekvensen de overvåker, i to påfølgende kvartaler overstiger referansebedragerifrekvensen som gjelder for dette betalingsinstrumentet eller denne typen betalingstransaksjon i nevnte terskelverdiintervall for unntak.

3. Etter at betalingstjenesteytere har sluttet å gjøre bruk av unntaket omhandlet i artikkel 18 i samsvar med nr. 2 i denne artikkelen, skal de ikke bruke dette unntaket igjen før deres beregnede bedragerifrekvens i løpet av et kvartal er lik eller lavere enn referansebedragerifrekvensen for denne typen betalingstransaksjon i nevnte terskelverdiintervall.

4. Dersom betalingstjenesteytere igjen har til hensikt å gjøre bruk av unntaket omhandlet i artikkel 18, skal de underrette vedkommende myndigheter i god tid, og før de på ny gjør bruk av unntaket, skal de framlegge dokumentasjon på at deres overvåkede bedragerifrekvens er i samsvar med gjeldende referansebedragerifrekvens for nevnte terskelverdiintervall for unntak i samsvar med nr. 3 i denne artikkelen.

Artikkel 21

Overvåking

1. For å kunne gjøre bruk av unntakene omhandlet i artikkel 10–18 skal betalingstjenesteytere minst hvert kvartal registrere og overvåke følgende data for hver type betalingstransaksjon, med en inndeling i både fjernbetalingstransaksjoner og ikke-fjernbetalingstransaksjoner:

a) Samlet verdi av uautoriserte eller bedragerske betalingstransaksjoner i samsvar med artikkel 64 nr. 2 i direktiv (EU) 2015/2366, samlet verdi av alle betalingstransaksjoner og bedragerifrekvensen som følger av dem, herunder en inndeling i betalingstransaksjoner initiert gjennom sterk kundeautentisering og omfattet av hvert av unntakene.

b) Den gjennomsnittlige transaksjonsverdien, herunder en inndeling i betalingstransaksjoner initiert gjennom sterk kundeautentisering og omfattet av hvert av unntakene.

c) Antall betalingstransaksjoner der hvert av unntakene ble anvendt, og den prosentdelen de utgjør i forhold til samlet antall betalingstransaksjoner.

2. Betalingstjenesteytere skal gjøre resultatene av overvåkingen i henhold til nr. 1 tilgjengelig for vedkommende myndigheter og EBA, med forhåndsmelding til relevante vedkommende myndigheter på anmodning.

KAPITTEL IV

FORTROLIGHETEN OG INTEGRITETEN TIL BETALINGSTJENESTEBRUKERNES PERSONALISERTE SIKKERHETSOPPLYSNINGER

Artikkel 22

Generelle krav

1. Betalingstjenesteytere skal sikre fortroligheten og integriteten til betalingstjenestebrukernes personaliserte sikkerhets-opplysninger, herunder autentiseringskoder, i alle faser av autentiseringen.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere sikre at alle følgende krav oppfylles:

a) Personaliserte sikkerhetsopplysninger maskeres når de vises, og de kan ikke leses i sin helhet når de angis av betalingstjenestebrukeren under autentiseringen.

b) Personaliserte sikkerhetsopplysninger i dataformat samt kryptografisk materiale knyttet til krypteringen av personaliserte sikkerhetsopplysninger lagres ikke i klartekst.

c) Hemmelig kryptografisk materiale er beskyttet mot uautorisert offentliggjøring.

3. Betalingstjenesteytere skal fullt ut dokumentere prosessen knyttet til håndteringen av kryptografisk materiale som brukes til å kryptere de personaliserte sikkerhetsopplysningene eller på annen måte gjøre dem uleselige.

4. Betalingstjenesteytere skal sikre at behandlingen og rutingen av personaliserte sikkerhetsopplysninger og autentiseringskoder som genereres i samsvar med kapittel II, foregår i et sikkert miljø i samsvar med robuste og allment anerkjente bransjestandarder.

Artikkel 23

Opprettelse og overføring av sikkerhetsopplysninger

Betalingstjenesteytere skal sikre at opprettelsen av personaliserte sikkerhetsopplysninger skjer i et sikkert miljø.

De skal redusere risikoen for uautorisert bruk av de personaliserte sikkerhetsopplysningene og av autentiseringsenheter og programvaren ved tap, tyveri eller kopiering før de leveres til betaleren.

Artikkel 24

Forbindelse med betalingstjenestebrukeren

1. Betalingstjenesteytere skal sikre at bare betalingstjenestebrukeren på en sikker måte er forbundet med de personaliserte sikkerhetsopplysningene, autentiseringsenhetene og programvaren.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere sikre at alle følgende krav oppfylles:

a) Forbindelsen mellom betalingstjenestebrukerens identitet og de personaliserte sikkerhetsopplysningene, autentiseringsenhetene og programvaren skjer på betalingstjenesteyterens ansvar i et sikkert miljø som minst omfatter betalingstjenesteyterens lokaler, internettmiljøet som betalingstjenesteyteren stiller til rådighet, eller andre lignende sikre nettsteder som brukes av betalingstjenesteyteren, samt dennes kontantautomattjenester, idet det tas hensyn til risikoene knyttet til enheter og underliggende komponenter som brukes under forbindelsesprosessen, og som betalingstjenesteyteren ikke er ansvarlig for.

b) Forbindelsen via en fjernkanal mellom betalingstjenestebrukerens identitet og de personaliserte sikkerhetsopplysningene, autentiseringsenhetene eller programvaren skjer ved hjelp av sterk kundeautentisering.

Artikkel 25

Levering av sikkerhetsopplysninger, autentiseringsenheter og programvare

1. Betalingstjenesteytere skal sikre at leveringen av personaliserte sikkerhetsopplysninger, autentiseringsenheter og programvare til betalingstjenestebrukeren skjer på en sikker måte som kan håndtere risikoene knyttet til uautorisert bruk som skyldes tap, tyveri og kopiering.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere minst anvende alle følgende tiltak:

a) Effektive og sikre leveringsordninger som sørger for at de personaliserte sikkerhetsopplysningene, autentiseringsenhetene og programvaren leveres til den rettmessige betalingstjenestebrukeren.

b) Ordninger som gjør at betalingstjenesteyteren kan kontrollere ektheten til autentiseringsprogramvaren som leveres til betalingstjenestebrukeren via internett.

c) Ordninger som sikrer følgende dersom leveringen av de personaliserte sikkerhetsopplysningene gjennomføres utenfor betalingstjenesteyterens lokaler eller via en fjernkanal:

   i) Ingen uautoriserte parter kan innhente mer enn ett enkelt element av de personaliserte sikkerhetsopplysningene, autentiseringsenhetene eller programvaren når de leveres gjennom samme kanal.

   ii) Personaliserte sikkerhetsopplysninger, autentiseringsenheter eller programvare som er levert, krever aktivering før bruk.

d) Dersom de personaliserte sikkerhetsopplysningene, autentiseringsenhetene eller programvaren krever aktivering før bruk, kreves ordninger som sikrer at aktiveringen skjer i et sikkert miljø i samsvar med forbindelsesprosedyrene omhandlet i artikkel 24.

Artikkel 26

Fornyelse av personaliserte sikkerhetsopplysninger

Betalingstjenesteytere skal sikre at fornyelse eller reaktivering av personaliserte sikkerhetsopplysninger følger framgangsmåtene for opprettelse av, forbindelse med og levering av sikkerhetsopplysninger og autentiseringsenheter i samsvar med artikkel 23, 24 og 25.

Artikkel 27

Tilintetgjøring, deaktivering og tilbakekalling

Betalingstjenesteytere skal sikre at de har effektive prosesser på plass for å treffe alle følgende sikkerhetstiltak:

a) Sikker tilintetgjøring, deaktivering eller tilbakekalling av de personaliserte sikkerhetsopplysningene, autentiseringsenhetene og programvaren.

b) Dersom betalingstjenesteyteren distribuerer autentiseringsenheter og programvare som kan gjenbrukes, er sikker gjenbruk av en enhet eller programvare etablert, dokumentert og gjennomført før enheten eller programvaren stilles til rådighet for en annen betalingstjenestebruker.

c) Deaktivering eller tilbakekalling av informasjon knyttet til personaliserte sikkerhetsopplysninger lagret i betalingstjenesteyterens systemer og databaser og eventuelt i offentlige transaksjonsregistre.

KAPITTEL V

FELLES OG SIKRE ÅPNE KOMMUNIKASJONSSTANDARDER

Avsnitt 1

Generelle kommunikasjonskrav

Artikkel 28

Identifiseringskrav

1. Betalingstjenesteytere skal sørge for sikker identifisering ved kommunikasjon mellom betalerens enhet og betalingsmottakerens godkjenningsenheter for elektroniske betalinger, herunder, men ikke begrenset til, betalingsterminaler.

2. Betalingstjenesteytere skal sørge for at risikoen for feildirigering av kommunikasjon til uautoriserte parter i mobile applikasjoner og andre betalingstjenestebrukergrensesnitt som tilbyr elektroniske betalingstjenester, på en effektiv måte reduseres.

Artikkel 29

Sporbarhet

1. Betalingstjenesteytere skal ha innført prosesser som sikrer at alle betalingstransaksjoner og andre interaksjoner med betalingstjenestebrukere, andre betalingstjenesteytere og andre enheter, herunder forretningsdrivende, i forbindelse med levering av betalingstjenesten er sporbare, noe som sikrer etterfølgende kjennskap til alle hendelser som er relevante for den elektroniske transaksjonen i alle dens stadier.

2. Ved anvendelse av nr. 1 skal betalingstjenesteytere sikre at alle kommunikasjonssesjoner med betalingstjenestebrukeren, andre betalingstjenesteytere og andre enheter, herunder forretningsdrivende, bygger på følgende:

a) En entydig identifikator for sesjonen.

b) Sikkerhetsordninger for detaljert registrering av transaksjonen, herunder transaksjonsnummer, tidsstempler og alle relevante transaksjonsdata.

c) Tidsstempler som skal bygge på et felles tidsreferansesystem, og som er synkronisert med et offisielt tidssignal.

Avsnitt 2

Særskilte krav til felles og sikre åpne kommunikasjonsstandarder

Artikkel 30

Generelle forpliktelser for tilgangsgrensesnitt

1. Kontotilbydere som tilbyr en betaler en betalingskonto som er tilgjengelig over nett, skal ha minst ett grensesnitt som oppfyller alle følgende krav:

a) Ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, kan identifisere seg overfor kontotilbyderen.

b) Ytere av kontoopplysningstjenester kan kommunisere sikkert for å anmode om og motta opplysninger om én eller flere utpekte betalingskontoer og tilhørende betalingstransaksjoner.

c) Ytere av betalingsinitieringstjenester kan kommunisere sikkert for å initiere en betalingsordre fra betalerens betalingskonto og motta alle opplysninger om initieringen av betalingstransaksjonen og alle opplysninger som er tilgjengelige for kontotilbyderen med hensyn til utførelsen av betalingstransaksjonen.

2. Ved autentisering av betalingstjenestebrukeren skal grensesnittet omhandlet i nr. 1 tillate ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester å bruke alle autentiseringsprosedyrene som kontotilbyderen stiller til rådighet for betalingstjenestebrukeren.

Grensesnittet skal minst oppfylle alle følgende krav:

a) En yter av betalingsinitieringstjenester eller en yter av kontoopplysningstjenester skal kunne pålegge kontotilbyderen å starte autentiseringen basert på betalingstjenestebrukerens samtykke.

b) Kommunikasjonssesjoner mellom kontotilbyderen, yteren av kontoopplysningstjenester, yteren av betalingsinitieringstjenester og berørte betalingstjenestebrukere skal opprettes og opprettholdes gjennom hele autentiseringen.

c) Integriteten og fortroligheten til de personaliserte sikkerhetsopplysningene og autentiseringskodene som overføres av eller gjennom yteren av betalingsinitieringstjenester eller yteren av kontoopplysningstjenester, skal sikres.

3. Kontotilbydere skal sikre at deres grensesnitt følger kommunikasjonsstandarder utstedt av internasjonale eller europeiske standardiseringsorganisasjoner.

Kontotilbydere skal også sikre at de tekniske spesifikasjonene for alle grensesnitt er dokumentert, med avgivelse av et sett med rutiner, protokoller og verktøy som ytere av betalingsinitieringstjenester, ytere av kontoopplysningstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, trenger for at deres programvare og applikasjoner skal kunne fungere sammen med kontotilbydernes systemer.

Kontotilbydere skal som et minimum, og minst seks måneder før anvendelsesdatoen angitt i artikkel 38 nr. 2, eller før måldatoen for markedslanseringen av tilgangsgrensesnittet dersom lanseringen finner sted etter datoen omhandlet i artikkel 38 nr. 2, gjøre dokumentasjonen kostnadsfritt tilgjengelig på anmodning fra godkjente ytere av betalingsinitieringstjenester, ytere av kontoopplysningstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, eller betalingstjenesteytere som har søkt sine vedkommende myndigheter om relevant tillatelse, og skal gjøre et sammendrag av dokumentasjonen offentlig tilgjengelig på sitt nettsted.

4. I tillegg til det som er angitt i nr. 3, skal kontotilbydere, unntatt i krisesituasjoner, sikre at eventuelle endringer i grensesnittenes tekniske spesifikasjoner gjøres tilgjengelig for godkjente ytere av betalingsinitieringstjenester, ytere av kontoopplysningstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, eller betalingstjenesteytere som har søkt sine vedkommende myndigheter om relevant tillatelse, på forhånd så snart som mulig og senest tre måneder før endringen gjennomføres.

Betalingstjenesteytere skal dokumentere krisesituasjoner der endringer ble gjennomført, og skal gjøre dokumentasjonen tilgjengelig for vedkommende myndigheter på anmodning.

5. Kontotilbydere skal stille til rådighet en testinnretning, herunder støttetjenester, for tilkoblings- og funksjonstesting, slik at godkjente ytere av betalingsinitieringstjenester, ytere av kontoopplysningstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, eller betalingstjenesteytere som har søkt sine vedkommende myndigheter om relevant tillatelse, kan teste den programvaren og de applikasjonene som benyttes for å tilby brukerne en betalingstjeneste. Testinnretningen skal gjøres tilgjengelig senest seks måneder før anvendelsesdatoen angitt i artikkel 38 nr. 2, eller før måldatoen for markedslanseringen av tilgangsgrensesnittet dersom lanseringen finner sted etter datoen omhandlet i artikkel 38 nr. 2.

Sensitiv informasjon kan imidlertid ikke deles gjennom testinnretningen.

6. Vedkommende myndigheter skal sikre at kontotilbydere til enhver tid oppfyller forpliktelsene som inngår i disse standardene, med hensyn til grensesnittene som benyttes. Dersom en kontotilbyder ikke oppfyller kravene for grensesnitt som er angitt i disse standardene, skal vedkommende myndigheter sikre at leveringen av betalingsinitieringstjenester og kontoopplysningstjenester ikke hindres eller forstyrres, i den grad de respektive yterne av slike tjenester oppfyller vilkårene i artikkel 33 nr. 5.

Artikkel 31

Alternativer for tilgangsgrensesnitt

Kontotilbydere skal opprette grensesnittene omhandlet i artikkel 30 ved å benytte enten et særskilt grensesnitt eller ved å tillate at betalingstjenesteyterne nevnt i artikkel 30 nr. 1 bruker grensesnittene for autentisering av og kommunikasjon med kontotilbyderens betalingstjenestebrukere.

Artikkel 32

Forpliktelser med hensyn til et særskilt grensesnitt

1. Med forbehold for overholdelse av artikkel 30 og 31 skal kontotilbydere som har innført et særskilt grensesnitt, sikre at dette grensesnittet til enhver tid har samme tilgjengelighet og ytelse, herunder støttetjenester, som grensesnittene som stilles til rådighet for betalingstjenestebrukeren for direkte nettbasert tilgang til dennes betalingskonto.

2. Kontotilbydere som har innført et særskilt grensesnitt, skal fastsette transparente sentrale ytelsesindikatorer og servicenivåmål som er minst like strenge som dem fastsatt for grensesnittet brukt av deres betalingstjenestebrukere, med hensyn til tilgjengelighet og levering av data i samsvar med artikkel 36. Disse grensesnittene, indikatorene og målene skal overvåkes av vedkommende myndigheter og stresstestes.

3. Kontotilbydere som har innført et særskilt grensesnitt, skal sikre at dette grensesnittet ikke skaper hindringer for leveringen av betalingsinitieringstjenester og kontoopplysningstjenester. Slike hindringer kan blant annet være at betalingstjenesteyterne omhandlet i artikkel 30 nr. 1 hindres i å bruke sikkerhetsopplysningene som kontotilbydere har utstedt for sine kunder, innføring av omdirigering til kontotilbyderens autentisering eller andre funksjoner, krav om ytterligere autentisering og registrering i tillegg til det som er angitt i artikkel 11, 14 og 15 i direktiv (EU) 2015/2366, eller krav om ytterligere kontroll av samtykket gitt av betalingstjenestebrukere til ytere av betalingsinitieringstjenester og ytere av kontoopplysningstjenester.

4. Ved anvendelse av nr. 1 og 2 skal kontotilbydere overvåke det særskilte grensesnittets tilgjengelighet og ytelse. Kontotilbydere skal på sitt nettsted offentliggjøre kvartalsstatistikk over tilgjengelighet og ytelse for det særskilte grensesnittet og for grensesnittet som brukes av deres betalingstjenestebrukere.

Artikkel 33

Beredskapstiltak for et særskilt grensesnitt

1. Kontotilbydere skal i utformingen av det særskilte grensesnittet inkludere en strategi og planer for beredskapstiltak for hendelser der grensesnittet ikke fungerer i samsvar med artikkel 32, der grensesnittet er uforutsett utilgjengelig, og der systemet har havarert. Den uforutsette utilgjengeligheten eller systemhavariet kan antas å ha inntruffet dersom fem påfølgende anmodninger om tilgang til opplysninger for å kunne levere betalingsinitieringstjenester eller kontoopplysningstjenester ikke blir besvart innen 30 sekunder.

2. Beredskapstiltakene skal omfatte kommunikasjonsplaner for å underrette betalingstjenesteytere som bruker det særskilte grensesnittet, om tiltak for å gjenopprette systemet og en beskrivelse av umiddelbart tilgjengelige alternative løsninger for betalingstjenesteytere i denne perioden.

3. Både kontotilbyderen og betalingstjenesteyterne omhandlet i artikkel 30 nr. 1 skal omgående rapportere om problemer med særskilte grensesnitt som beskrevet i nr. 1 til sine respektive nasjonale vedkommende myndigheter.

4. Som del av en beredskapsordning skal betalingstjenesteytere omhandlet i artikkel 30 nr. 1 ha mulighet til å bruke grensesnittene som gjøres tilgjengelige for betalingstjenestebrukere for autentisering av og kommunikasjon med deres kontotilbydere, inntil det særskilte grensesnittet er gjenopprettet til det tilgjengelighets- og ytelsesnivået som er fastsatt i artikkel 32.

5. For dette formål skal kontotilbydere sikre at betalingstjenesteyterne omhandlet i artikkel 30 nr. 1 kan identifiseres, og at de kan bruke autentiseringsprosedyrene som kontotilbyderen stiller til rådighet for betalingstjenestebrukeren. Dersom betalingstjenesteyterne omhandlet i artikkel 30 nr. 1 gjør bruk av grensesnittet nevnt i nr. 4, skal de

a) treffe de nødvendige tiltakene for å sikre at de ikke henter, lagrer eller behandler data for andre formål enn levering av tjenesten som betalingstjenestebrukeren har anmodet om,

b) fortsette å overholde forpliktelsene som følger av artikkel 66 nr. 3 og artikkel 67 nr. 2 i direktiv (EU) 2015/2366,

c) logge dataene de får tilgang til gjennom grensesnittet som kontotilbyderen stiller til rådighet for sine betalingstjenestebrukere, og på anmodning og uten utilbørlig forsinkelse levere loggfilene til sin vedkommende nasjonale myndighet,

d) på anmodning og uten utilbørlig forsinkelse behørig begrunne overfor sin vedkommende nasjonale myndighet bruken av grensesnittet som er gjort tilgjengelig for betalingstjenestebrukerne for direkte nettbasert tilgang til betalingskontoen,

e) informere kontotilbyderen om dette.

6. Vedkommende myndigheter skal, etter samråd med EBA for å sikre ensartet anvendelse av følgende forhold, unnta kontotilbydere som har valgt et særskilt grensesnitt, fra plikten til å opprette beredskapsordningen som er omhandlet i nr. 4, dersom det særskilte grensesnittet oppfyller alle følgende vilkår:

a) Det oppfyller alle forpliktelser for særskilte grensesnitt som omhandlet i artikkel 32.

b) Det er utformet og testet i samsvar med artikkel 30 nr. 5 på en måte som de nevnte betalingstjenesteyterne er tilfreds med.

c) Det er blitt brukt i stor utstrekning i minst tre måneder av betalingstjenesteytere for å tilby kontoopplysningstjenester og betalingsinitieringstjenester og for å bekrefte tilgjengelige midler ved kortbaserte betalinger.

d) Ethvert problem knyttet til det særskilte grensesnittet er blitt løst uten utilbørlig forsinkelse.

7. Vedkommende myndigheter skal tilbakekalle unntaket omhandlet i nr. 6 dersom kontotilbyderne i mer enn to påfølgende kalenderuker ikke har oppfylt vilkårene i bokstav a) og d). Vedkommende myndigheter skal underrette EBA om denne tilbakekallingen og sikre at kontotilbyderen snarest mulig og senest i løpet av to måneder oppretter beredskapsordningen omhandlet i nr. 4.

Artikkel 34

Sertifikater

1. Med hensyn til identifisering som omhandlet i artikkel 30 nr. 1 bokstav a) skal betalingstjenesteytere benytte kvalifiserte sertifikater for elektroniske segl som nevnt i artikkel 3 nr. 30 i forordning (EU) nr. 910/2014 eller for nettstedsautentisering som nevnt i artikkel 3 nr. 39 i nevnte forordning.

2. Ved anvendelse av denne forordningen skal registreringsnummeret som det vises til i offisielle registre i samsvar med bokstav c) i vedlegg III eller bokstav c) i vedlegg IV til forordning (EU) nr. 910/2014, være tillatelsesnummeret til betalingstjenesteyteren som utsteder kortbaserte betalingsinstrumenter, ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester, herunder kontotilbydere som tilbyr slike tjenester, som finnes i det offentlige registeret i hjemstaten i henhold til artikkel 14 i direktiv (EU) 2015/2366, eller som følger av underretninger om alle tillatelser gitt i henhold til artikkel 8 i europaparlaments- og rådsdirektiv 2013/36/EU([1]) i samsvar med artikkel 20 i nevnte direktiv.

3. Ved anvendelse av denne forordningen skal kvalifiserte sertifikater for elektroniske segl eller for nettstedsautentisering som nevnt i nr. 1 omfatte, på et språk som er vanlig i internasjonale finanskretser, særskilte tilleggskjennetegn for hvert av følgende:

a) Betalingstjenesteyterens rolle, som kan være én eller flere av følgende:

   i) Kontoforvaltning.

   ii) Betalingsinitiering.

   iii) Kontoopplysninger.

   iv) Utstedelse av kortbaserte betalingsinstrumenter.

b) Navnet på vedkommende myndigheter der betalingstjenesteyteren er registrert.

4. Kjennetegnene nevnt i nr. 3 skal ikke påvirke samvirkingsevnen til og anerkjennelsen av kvalifiserte sertifikater for elektroniske segl eller nettstedsautentisering.

([1]) Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet som kredittinstitusjon og om tilsyn med kredittinstitusjoner og verdipapirforetak, om endring av direktiv 2002/87/EF og om oppheving av direktiv 2006/48/EF og 2006/49/EF (EUT L 176 av 27.6.2013, s. 338).

Artikkel 35

Sikre kommunikasjonssesjoner

1. Kontotilbydere, betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester skal, når de utveksler opplysninger via internett, sørge for at det anvendes sikker kryptering mellom de kommuniserende partene i hele den aktuelle kommunikasjonssesjonen med bruk av sterke og allment anerkjente krypteringsteknikker for å sikre dataenes fortrolighet og integritet.

2. Betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester skal holde tilgangssesjonen som tilbys av kontotilbyderen, så kort som mulig, og de skal aktivt avslutte slike sesjoner så snart handlingen det er anmodet om, er fullført.

3. Når ytere av kontoopplysningstjenester og ytere av betalingsinitieringstjenester har parallelle nettverkssesjoner med kontotilbyderen, skal de sørge for at disse sesjonene er forsvarlig knyttet til relevante sesjoner med betalingstjenestebrukere, for å forhindre at eventuelle meldinger eller opplysninger som utveksles mellom dem, kan bli feildirigert.

4. Ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, skal i kommunikasjonen med kontotilbyderen ha utvetydige henvisninger til hver av følgende:

a) Betalingstjenestebrukeren eller -brukerne og tilhørende kommunikasjonssesjon for å skille mellom flere anmodninger fra samme betalingstjenestebrukere.

b) For betalingsinitieringstjenester, den entydig identifiserte betalingstransaksjonen som er initiert.

c) For bekreftelse av tilgjengelige midler, den entydig identifiserte anmodningen knyttet til beløpet som kreves for å utføre den kortbaserte betalingstransaksjonen.

5. Kontotilbydere, ytere av kontoopplysningstjenester, ytere av betalingsinitieringstjenester og betalingstjenesteytere som utsteder kortbaserte betalingsinstrumenter, skal, dersom de oversender personaliserte sikkerhetsopplysninger og autentiseringskoder, sikre at disse aldri er leselige, verken direkte eller indirekte, for personalet.

Dersom de personaliserte sikkerhetsopplysningene mister sin fortrolighet mens de er tilbydernes eller tjenesteyternes ansvar, skal disse uten utilbørlig forsinkelse underrette betalingstjenestebrukeren forbundet med dem og utstederen av de personlige sikkerhetsopplysningene.

Artikkel 36

Datautveksling

1. Kontotilbydere skal oppfylle alle følgende krav:

a) De skal gi ytere av kontoopplysningstjenester de samme opplysningene fra utpekte betalingskontoer og tilhørende betalingstransaksjoner som gjøres tilgjengelige for betalingstjenestebrukeren ved direkte anmodning om tilgang til kontoopplysningene, forutsatt at disse opplysningene ikke omfatter sensitiv betalingsinformasjon.

b) De skal umiddelbart etter mottak av betalingsordren gi ytere av betalingsinitieringstjenester de samme opplysningene om initieringen og utførelsen av betalingstransaksjonen som gis til eller gjøres tilgjengelig for betalingstjenestebrukeren, når transaksjonen initieres direkte av sistnevnte.

c) De skal på anmodning umiddelbart gi betalingstjenesteytere en bekreftelse i et enkelt ja- eller nei-format om beløpet som kreves for å utføre en betalingstransaksjon, er tilgjengelig på betalerens betalingskonto.

2. Ved en uforutsett hendelse eller feil som oppstår i forbindelse med identifiserings- eller autentiseringsprosessen eller utvekslingen av dataelementer, skal kontotilbyderen sende en melding til yteren av betalingsinitieringstjenester eller yteren av kontoopplysningstjenester og betalingstjenesteyteren som utsteder kortbaserte betalingsinstrumenter, som forklarer årsaken til den uforutsette hendelsen eller feilen.

Dersom kontotilbyderen stiller et særskilt grensesnitt til rådighet i samsvar med artikkel 32, skal grensesnittet sørge for at meldinger om uforutsette hendelser eller feil formidles av enhver betalingstjenesteyter som oppdager hendelsen eller feilen, til de andre betalingstjenesteyterne som deltar i kommunikasjonssesjonen.

3. Ytere av kontoopplysningstjenester skal ha innført egnede og effektive ordninger som hindrer tilgang til andre opplysninger enn fra utpekte betalingskontoer og tilhørende betalingstransaksjoner, i samsvar med brukerens uttrykkelige samtykke.

4. Ytere av betalingsinitieringstjenester skal gi kontotilbydere de samme opplysningene som det anmodes om fra betalingstjenestebrukeren ved direkte initiering av betalingstransaksjonen.

5. Ytere av kontoopplysningstjenester skal ha tilgang til opplysninger fra utpekte betalingskontoer og tilhørende betalingstransaksjoner som innehas av kontotilbydere, for å utføre kontoopplysningstjenesten under følgende omstendigheter:

a) Når betalingstjenestebrukeren aktivt anmoder om slike opplysninger.

b) Dersom betalingstjenestebrukeren ikke aktivt anmoder om slike opplysninger, høyst fire ganger i løpet av en 24-timersperiode, med mindre en større hyppighet er avtalt mellom yteren av kontoopplysningstjenester og kontotilbyderen, med betalingstjenestebrukerens samtykke.

KAPITTEL VI

SLUTTBESTEMMELSER

Artikkel 37

Gjennomgåelse

Uten at det berører artikkel 98 nr. 5 i direktiv (EU) 2015/2366, skal EBA senest 14. mars 2021 gjennomgå bedragerifrekvensene angitt i vedlegget til denne forordningen samt unntakene gitt i henhold til artikkel 33 nr. 6 i forbindelse med særskilte grensesnitt, og skal eventuelt framlegge utkast til oppdateringer av disse for Kommisjonen i samsvar med artikkel 10 i forordning (EU) nr. 1093/2010.

Artikkel 38

Ikrafttredelse

1. Denne forordningen trer i kraft dagen etter at den er kunngjort i *Den europeiske unions tidende.*

2. Denne forordningen får anvendelse fra 14. september 2019.

3. Artikkel 30 nr. 3 og 5 får imidlertid anvendelse fra 14. mars 2019.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 27. november 2017.

For Kommisjonen

Jean-Claude JUNCKER

President

VEDLEGG

	Referansebedragerifrekvens (%) for	
Terskelverdi for unntak (ETV)	Elektroniske kortbaserte fjernbetalinger	Elektroniske fjernkreditoverføringer
500 euro	0,01	0,005
250 euro	0,06	0,01
100 euro	0,13	0,015