Remisspromemoria

Datum 2021-12-01 FI dnr 21-23860

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Förslag till ändringar i föreskrifter om rapportering vid allvarliga incidenter

Sammanfattning

Finansinspektionen föreslår ändringar i Finansinspektionens föreskrifter (FFFS 2018:4) om verksamhet för betaltjänstleverantörer. Ändringarna rör incidentrapportering och är föranledda av att Europeiska bankmyndigheten (EBA) har reviderat sin riktlinje för rapportering vid allvarliga incidenter enligt andra betaltjänstdirektivet. Syftet med förslaget är att säkerställa att endast relevanta incidenter, det vill säga sådana som kan klassificeras som allvarliga, rapporteras till Finansinspektionen. Förslaget syftar också till att säkerställa att inspektionen får del av relevant information om de grundläggande orsakerna till incidenterna samt vilka åtgärder företagen avser att vidta för att undvika upprepning av inträffade allvarliga incidenter.

Ändringarna i föreskrifterna föreslås träda i kraft den 1 april 2022.

Innehåll

1 Utgångspunkter

1.1 Bakgrund och målet med regleringen

Finansinspektionen föreslår att vissa bestämmelser om incidentrapportering i Finansinspektionens föreskrifter (FFFS 2018:4) om verksamhet för betaltjänstleverantörer (betaltjänstföreskrifterna) ändras.

Betaltjänstföreskrifterna har sin grund i EU:s andra betaltjänstdirektiv[1] (PSD2 eller andra betaltjänstdirektivet) som reglerar konton och betalningar för både företag och privatpersoner. Den Europeiska bankmyndigheten (EBA) har i anslutning till PSD2 beslutat om riktlinjer som syftar till att nå en konsekvent hantering av de frågor som regleras i direktivet. En sådan riktlinje gäller rapportering vid allvarliga incidenter.[2]

Finansinspektionens anser generellt att riktlinjer från EBA och de andra europeiska tillsynsmyndigheterna gäller som svenska allmänna råd. Inspektionen har dock möjlighet att välja att göra om delar av en riktlinje till bindande föreskrifter. När betaltjänstföreskrifterna beslutades 2018 valde inspektionen att föra in delar av EBA:s riktlinje för rapportering vid allvarliga incidenter i föreskrifterna.

EBA initierade under 2020 en översyn av denna riktlinje. Målsättningen med översynen var både att förenkla rapporteringen av incidenter under PSD2, fånga it-säkerhetsrelaterade incidenter i rapporteringen och minska antalet operationella incidenter som rapporterades. Den reviderade riktlinjen[3] beslutades den 10 juni 2021 och gäller från den 1 januari 2022.

På grund av de ändringar som görs i riktlinjen behöver även Finansinspektionens föreskrifter justeras på det sätt som närmare beskrivs i avsnitt 2.

De ändrade föreskrifterna föreslås träda i kraft den 1 april 2022.

[1] Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.
[2] Riktlinjer för rapportering vid allvarliga incidenter enligt direktiv (EU) 2015/2366 (andra betaltjänstdirektivet), EBA/GL/2017/10.
[3] Reviderade riktlinjer för rapportering vid allvarliga incidenter enligt andra betaltjänstdirektivet, EBA/GL/2021/03.

1.2 Nuvarande och kommande regelverk

Den övergripande regleringen för betaltjänstleverantörers verksamhet finns i lagen (2010:751) om betaltjänster (betaltjänstlagen). Därutöver finns bestämmelser som berör leverantörernas verksamhet i bland annat Finansinspektionens föreskrifter och allmänna råd (FFFS 2010:3) om betalningsinstitut och registrerade betaltjänstleverantörer samt i betaltjänstföreskrifterna.

Det pågår ett arbete inom EU med att ta fram och besluta om en förordning om digital operativ motståndskraft i den finansiella sektorn[4] (DORA)[5]. I förordningen finns bestämmelser om uppföljning och rapportering av eventuella informations- och kommunikationsrelaterade (IKT) incidenter i syfte att hantera dem på ett adekvat sätt samt tillvara erfarenheter och identifiera vilka förbättringar som behöver genomföras. De europeiska tillsynsmyndigheterna ska i samråd med EU:s datasäkerhetsmyndighet (Enisa) ta fram tekniska standarder med mer detaljerade regler om riskhantering och riskramverket.

EBA har valt att trots detta arbete revidera riktlinjen för rapportering vid allvarliga incidenter enligt PSD2, då riktlinjen bedöms kunna vara i kraft en tillräckligt lång tid innan de nya tekniska standarderna för rapportering enligt DORA beräknas vara på plats. När de nya tekniska standarderna väl beslutas kommer betaltjänstföreskrifterna behöva ses över igen.

1.3 Regleringsalternativ

Finansinspektionen avser att följa den reviderade riktlinjen från EBA. De föreslagna ändringarna i föreskrifterna är nödvändiga för att riktlinjerna och föreskrifterna inte ska strida mot varandra.

Ett alternativ till att ändra föreskrifterna skulle kunna vara att upphäva föreskrifterna i denna del och låta riktlinjen i sin helhet gälla på samma sätt som allmänna råd. Det bedöms dock inte vara ett lämpligt alternativ eftersom styrningen då blir svagare än om regleringen sker genom föreskrifter. Finansinspektionen skulle då inte heller ha samma möjlighet att bedriva tillsyn över företag som rapporterar allvarliga operativa incidenter och säkerhetsincidenter på fel sätt. Detta skulle i sin tur påverka

[4] Förslag till EU-parlamentets och rådets förordning om digital operativ motståndskraft i den finansiella sektorn och ändring av förordning (EU) 1060/2012, (EU) 600/2014 och (EU) 909/2014.
[5] EU regulatory framework on digital operational resilience.

Finansinspektionens möjlighet att fullgöra sin skyldighet enligt 5 b kap. 3 § betaltjänstlagen att informera Riksbanken, andra berörda svenska myndigheter, Europeiska bankmyndigheten och Europeiska centralbanken, om dessa incidenter.

1.4 Rättsliga förutsättningar

En betaltjänstleverantör ska enligt 5 b kap. 1 § betaltjänstlagen ha ett system med lämpliga åtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker som är förknippade med de betaltjänster som den tillhandahåller. Inom ramen för detta system ska betaltjänstleverantören reglera hur den ska hantera incidenter. I 5 b kap. 3 § första stycket betaltjänstlagen anges att en betaltjänstleverantör så snart det kan ske ska underrätta Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident som uppkommit i verksamheten. Enligt 5 b kap. 6 § 1 betaltjänstlagen får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om hur ett system enligt 1 § ska utformas. Regeringen har genom 5 § 13 förordningen (2010:1008) om betaltjänster bemyndigat Finansinspektionen att meddela föreskrifter om detta.

Som inspektionen angav i den ursprungliga beslutspromemorian[6] till betaltjänstföreskrifterna utgör det förhållande att en betaltjänstleverantör ska underrätta Finansinspektionen om allvarliga incidenter en del av det system med åtgärder, kontrollmekanismer och interna regler som en sådan aktör ska ha enligt 5 b kap. 1 § betaltjänstlagen. Det är därför med stöd av bemyndigandet i 5 § 13 förordningen om betaltjänster som inspektionen föreskriver om hur och när underrättelserna ska lämnas till Finansinspektionen, och därmed gör de ändringar som nu föreslås.

1.5 Ärendets beredning

Finansinspektionen har bjudit in Svenska bankföreningen, Sparbankernas Riksförbund och Swedish Fintech Association att delta i en extern referensgrupp. På ett referensgruppsmöte den 18 oktober fick deltagarna i den externa referensgruppen möjlighet att lämna synpunkter på föreskriftsförslaget.

[6] Finansinspektionens beslutspromemoria, FI dnr. 15-10584, s.35.

2 Motivering och överväganden

Av 5 b kap. 3 § betaltjänstlagen framgår att en betaltjänstleverantör så snart det kan ske ska underrätta Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident uppkommit i verksamheten. I 6 kap. 4 § betaltjänstföreskrifterna finns närmare bestämmelser om hur denna rapportering ska gå till. I linje med de justeringar som görs i den reviderade riktlinjen bör bestämmelsen i 6 kap. 4 § betaltjänstföreskrifterna ändras.

När det gäller den inledande rapporten (avsnitt A i blanketten) innebär förslaget att den ska lämnas inom fyra timmar från den tidpunkt då den operativa incidenten eller säkerhetsincidenten klassificeras som allvarlig, i stället för som i dag fyra timmar efter att incidenten först upptäcktes. Syftet med ändringen är att säkerställa att endast relevanta incidenter, det vill säga sådana som kan klassificeras som allvarliga, rapporteras in till Finansinspektionen.

Förslaget innebär också att det tydliggörs att den mellanliggande rapporten (avsnitt B i blanketten) ska lämnas senast inom tre *arbets*dagar, i stället för som i dag inom tre dagar.

Därutöver innebär förslaget att slutrapporten (avsnitt C i blanketten) ska lämnas till Finansinspektionen senast 20 arbetsdagar efter det att driften anses vara normal igen, i stället för som i dag senast två veckor efter detta.

Övriga förändringar i den reviderade riktlinjen medför inga ändringar av Finansinspektionens föreskrifter. Den information och de mallar som rör rapporteringen som finns på Finansinspektionens webbplats kommer dock uppdateras så att de ligger i linje med riktlinjen.

3 Förslagets konsekvenser

3.1 Konsekvenser för samhället och konsumenterna

De föreslagna föreskriftsändringarna bedöms inte medföra ekonomiska eller andra konsekvenser för konsumenterna eller samhället.

3.2 Konsekvenser för företagen

Genom förslaget tydliggörs att det endast är operativa incidenter och säkerhetsincidenter som klassificerats som allvarliga som ska rapporteras till Finansinspektionen. Inspektionen bedömer att förslaget kommer innebära att incidenterna som rapporteras kommer att minska i jämförelse med vad som rapporteras enligt de nuvarande bestämmelserna. Det bedöms innebära en lättnad för företagen.

Det föreslås också att företagen får mer tid på sig att lämna slutrapporten, 20 arbetsdagar i stället för två veckor. Därutöver tydliggörs att den mellanliggande rapporten ska lämnas senast inom tre *arbets*dagar, i stället för som i dag inom tre dagar. Även det här bedömer inspektionen kommer att innebära en lättnad för företagen.

3.2.1 Berörda företag

Betaltjänstföreskrifterna gäller för följande betaltjänstleverantörer som tillhandahåller betaltjänster i Sverige

– kreditinstitut,
– betalningsinstitut,
– registrerade betaltjänstleverantörer,
– institut för elektroniska pengar, och
– registrerade utgivare av elektroniska pengar.

3.2.2 Kostnader för företagen

Förändringen bedöms inte medföra några ytterligare kostnader för företagen.

3.2.3 Konsekvenser för små företag

Förändringen kommer inte att medföra några särskilda konsekvenser för små företag.

3.3 Konsekvenser för Finansinspektionen

Finansinspektionen bedriver en riskbaserad tillsyn och incidentrapporter ger inspektionen en god inblick i hur betaltjänstleverantörer hanterar operativa risker och säkerhetsrisker. Genom att det nu tydliggörs att endast de operativa incidenterna och säkerhetsincidenterna som klassificeras som allvarliga ska rapporteras, förväntas antalet rapporterade incidenter minska.

Att tiden för slutrapporten förlängs från 2 veckor till 20 arbetsdagar, förväntas medföra att Finansinspektionen får ta del av mer relevant information om den grundläggande orsaken och vilka åtgärder företagen planerar för att undvika att allvarliga incidenter inträffar igen. Det bedöms sammantaget innebära att inspektionen får bättre underlag som kan ligga till grund för riskbedömning av betaltjänstleverantörernas verksamhet. I förlängningen underlättar detta för att bedöma vilka tillsynsåtgärder som behövs.

Därtill bedöms förändringarna sammantaget medföra att incidentrapporter som vidarerapporteras till EBA kommer att hålla en högre standard.

3.4 Tidpunkt för ikraftträdande

Med hänsyn till att förslagen inte innebär några stora förändringar för företagen bedömer Finansinspektionen att inga särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdandet, samt att det inte behövs några speciella informationsinsatser. Inspektionen kommer informera om förändringarna på Finansinspektionens webbplats.

3.5 Förenlighet med unionsrätten

Finansinspektionen bedömer att förslaget inte går utöver de skyldigheter som följer av Sveriges medlemskap i EU.