**Beslutspromemoria**

Datum 2022-03-15 FI dnr 21-23860

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

# Ändringar i föreskrifter om rapportering vid allvarliga incidenter

## Sammanfattning

Finansinspektionen ändrar i inspektionens föreskrifter (FFFS 2018:4) om verksamhet för betaltjänstleverantörer, som gäller för bland annat kreditinstitut och betalningsinstitut. Ändringarna, som träder i kraft den 1 april 2022, rör incidentrapportering.

Syftet med ändringarna är att säkerställa att endast relevanta incidenter, det vill säga sådana som kan klassificeras som allvarliga, rapporteras till Finansinspektionen. Ändringarna 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 att incidenterna upprepas.

Ändringarna är föranledda av att Europeiska bankmyndigheten (EBA) har uppdaterat sin riktlinje för rapportering vid allvarliga incidenter enligt det andra betaltjänstdirektivet.

# Innehåll

# 1 Utgångspunkter

## 1.1 Bakgrund och målet med regleringen

Finansinspektionen ändrar vissa bestämmelser om incidentrapportering i Finansinspektionens föreskrifter (FFFS 2018:4) om verksamhet för betaltjänstleverantörer (betaltjänstföreskrifterna). Föreskrifterna gäller för bland annat kreditinstitut och betalningsinstitut som tillhandahåller betaltjänster.

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

Finansinspektionen 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. Målet med översynen var både att förenkla rapporteringen av incidenter enligt PSD2, identifiera it-säkerhetsrelaterade incidenter i rapporteringen och minska antalet operativa incidenter som företagen rapporterade. Den uppdaterade riktlinjen[3] beslutades den 10 juni 2021 och gäller från den 1 januari 2022.

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

[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.

De ändrade föreskrifterna träder i kraft den 1 april 2022.

## 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 hur företagen ska följa upp och rapportera eventuella informations- och kommunikationsrelaterade incidenter. Syftet är att företagen ska hantera dem på ett adekvat sätt, ta tillvara erfarenheter och identifiera vilka förbättringar som behöver genomföras. De europeiska tillsynsmyndigheterna ska i samråd med EU:s datasäkerhetsmyndighet ta fram tekniska standarder med mer detaljerade regler om riskhantering och riskramverket.

Trots detta arbete har EBA valt att uppdatera riktlinjen för rapportering vid allvarliga incidenter enligt PSD2, eftersom 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 uppdaterade riktlinjen från EBA. Ändringarna i föreskrifterna är därför 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 gälla i sin helhet på samma sätt som allmänna råd. Det bedöms dock inte vara ett lämpligt alternativ eftersom styrningen då blir svagare än om regleringen sker genom

[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.

föreskrifter. Finansinspektionen skulle då inte heller ha samma möjlighet att utöva tillsyn över företag som rapporterar allvarliga operativa incidenter och säkerhetsincidenter på fel sätt. Det skulle i sin tur påverka Finansinspektionens möjlighet att fullgöra sin skyldighet enligt 5 b kap. 3 § betaltjänstlagen att informera Riksbanken, andra berörda svenska myndigheter, EBA 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 beslutas.

## 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 2021 fick deltagarna i den externa referensgruppen möjlighet att lämna synpunkter på föreskriftsförslaget.

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

Den 2 december 2021 remitterade Finansinspektionen ett förslag till ändringar i föreskrifterna. Sju remissinstanser har kommit in med svar och de har inte haft några invändningar mot förslaget. Tre privatpersoner har skrivit ett gemensamt remissvar. Vilka överväganden som inspektionen har gjort med anledning av de framförda remissynpunkterna framgår i avsnitt 2.

# 2 Motivering och överväganden

## 2.1 Föreskriftsändringar

**Finansinspektionens ställningstagande:** En betaltjänstleverantör ska rapportera en incident enligt 5 b kap. 3 § betaltjänstlagen

1. inom fyra timmar efter det att en operativ incident eller en säkerhetsincident har klassificerats som allvarlig (avsnitt A),

2. med uppdaterad information när det finns sådan och senast inom tre arbetsdagar från det att uppgifterna enligt 1 har kommit in (avsnitt B), och

3. senast 20 arbetsdagar efter det att verksamheten fungerar normalt igen (avsnitt C).

**Remisspromemorian:** Förslaget hade samma innehåll.

**Remissinstanserna:** Tillstyrker förslaget eller har inte haft något att invända mot det.

Tre *privatpersoner* har kommit in med ett gemensamt remissvar i vilket de har avstyrkt förslaget att ändra B-rapporten till tre arbetsdagar och C-rapporten till 20 arbetsdagar. De har därutöver rekommenderat att införa ett ytterligare förtydligande om tiden för klassificering av en incident.

**Finansinspektionens skäl:** 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 gjorts i den uppdaterade riktlinjen ändrar Finansinspektionen nu bestämmelsen i 6 kap. 4 § betaltjänstföreskrifterna.

Enligt den nya lydelsen ska den inledande rapporten (avsnitt A i blanketten) lämnas inom fyra timmar från den tidpunkt då den operativa incidenten eller säkerhetsincidenten klassificeras som allvarlig, i stället för som tidigare fyra timmar efter att incidenten upptäcktes. Syftet med ändringen är att säkerställa att företagen endast rapporterar relevanta incidenter till Finansinspektionen, det vill säga sådana som kan klassificeras som allvarliga.

Genom ändringarna tydliggörs också att den mellanliggande rapporten (avsnitt B i blanketten) ska lämnas senast inom tre arbetsdagar, i stället för som tidigare inom tre dagar.

Därutöver innebär ändringarna 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 tidigare senast två veckor efter detta.

Övriga förändringar i den uppdaterade riktlinjen medför inga ändringar i Finansinspektionens föreskrifter.

Några *privatpersoner* har i ett remissvar anfört att Finansinspektionen i stället för ”arbetsdagar” bör använda uttrycket ”bankdagar”, när det gäller inom vilken tid B- och C-rapporten ska lämnas in. Eftersom den engelska versionen av riktlinjen använder begreppet ”working days”, vilket är översatt till ”arbetsdagar” i den svenska versionen, anser dock Finansinspektionen att det är begreppet arbetsdagar som bör användas i föreskrifterna. Finansinspektionen ändrar därmed inte i förhållande till det remitterade förslaget. När det gäller privatpersonernas förslag om att det ska införas en ny bestämmelse i föreskrifterna som gäller tiden för klassificering av en incident, så har denna fråga inte beretts inom ramen för detta regelärende. Finansinspektionen noterar dessutom att förslaget skulle innebära att föreskrifterna går längre än vad riktlinjen anger. Finansinspektionen gör därför inte några ytterligare ändringar av föreskrifterna.

## 2.2 Ikraftträdande

**Finansinspektionen ställningstagande**: Ändringarna i föreskrifterna ska träda i kraft den 1 april 2022.

**Remisspromemorian:** Förslaget hade samma innehåll.

**Remissinstanserna**: Har inte haft något att invända mot förslaget.

**Finansinspektionens skäl:** Ändringarna är i huvudsak en följd av en uppdaterad EBA-riktlinje som redan har trätt i kraft. De bör därför börja gälla så snart som möjligt. Finansinspektionen beslutar därför att föreskriftsändringarna ska träda i kraft den 1 april 2022.

Eftersom de berörda företagen redan bör vara informerade om riktlinjen bedömer Finansinspektionen att det inte krävs några speciella informationsinsatser med anledning av föreskriftsändringarna.

# 3 Förslagets konsekvenser

## 3.1 Konsekvenser för samhället och konsumenterna

Föreskriftsändringarna bedöms inte medföra ekonomiska eller andra konsekvenser för konsumenterna eller samhället.

## 3.2 Konsekvenser för företagen

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

Genom ändringarna får företagen 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 arbetsdagar, i stället för som i dag inom tre dagar. Även detta 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

Ändringarna i föreskrifterna bedöms inte medföra några ytterligare kostnader för företagen.

### 3.2.3 Konsekvenser för små företag

Ändringarna i föreskrifterna 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 två 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 föreskriftsändringarna sammantaget medföra att incidentrapporter som rapporteras vidare till EBA kommer att hålla en högre standard.

## 3.4 Förenlighet med unionsrätten

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