Leiðbeiningar

um tilkynningu frávika

Eftirfarandi eru leiðbeiningar fjármálaeftirlits Seðlabanka Íslands (fjármálaeftirlitsins) vegna rafrænna tilkynninga um frávik í rekstri eftirlitsskyldra aðila. Frávikakerfið byggir á umgjörð sem gildir um frávik samkvæmt tilskipun (ESB) 2015/2366, um greiðsluþjónustu á innri markaðnum (PSD2) sem var innleidd með lögum 114/2021.

Hvað skal tilkynna

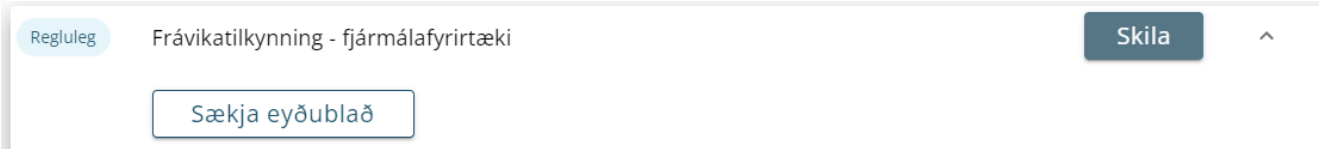
Tilkynna skal stærri frávik samkvæmt viðmiðum í neðangreindri töflu. Tilkynna skal frávik ef þrjú eða fleiri atriði í dálknum „Lægra viðmið" eiga við og/eða eitt atriði í dálknum „Hærra viðmið":

Skilyrði	Lægra viðmið	Hærra viðmið
Hlutfall mikilvægar þjónustu sem varð fyrir áhrifum	>5% af venjulegu umfangi þjónustu og lengd atviks > 1 klst **eða** > 1,5 m.kr og lengd atviks > 1 klst	>10% af venjulegu umfangi þjónustu **eða** > 50 m.kr.
Fjöldi notenda sem urðu fyrir áhrifum	> 500 og lengd atviks > 1 klst **eða** > 5% af notendum mikilv. þjónustu og lengd atviks > 1 klst	> 5.000 eða > 10% af notendum mikilv. þjónustu
Niðritími þjónustu	> 2 klst	
Brot á öryggisráðstöfunum	Já	
Fjárhagsleg áhrif fráviks		> 50 m.kr.
Stigmögnun viðbragða[1]		Já og líklegt að neyðaráætlun verði virkjuð
Áhrif á aðra EA eða mikilvæga innviði	Já	
Áhrif á orðspor	Já	
Leiðir atvikið til brots á lögum[2]		Já

Framkvæmd

Stærri frávik í rekstri eftirlitsskyldra aðila skal tilkynna til fjármálaeftirlitsins í gagnaskilakerfi Seðlabankans: https://gagnaskil.sedlabanki.is/[3]

Athugið að ef um sérlega alvarlegt atvik er að ræða ber að hringja fyrst í snr. 665 7777
Þar er að finna frávikaskráningarform sem nota skal við tilkynningar.



Hvert stærra frávik skal tilkynna í þrennu lagi og í öll skiptin nota sama skjalið. Þeir aðilar sem falla undir lög nr. 114/2021 um greiðsluþjónustu (PSD2) skulu fylla formið út á ensku, en valfrjálst er fyrir aðra eftirlitsskylda aðila hvort þeir noti ensku eða íslensku við útfyllinguna. Framkvæmdin skal vera eftirfarandi:

[1] Ef fráviki er flaggað við framkvæmdastjóra eða efsta lag stjórnenda.

[2] Leiði frávik í rekstri eftirlitsskylds aðila til þess að aðilinn geti ekki uppfyllt kröfur laga sem eiga við um starfsemina skal senda tilkynningu. Dæmi um slíkt gæti verið tilfelli þar sem stöðvun tölvukerfis leiðir til þess að lögbundin skýrsluskil berist ekki til eftirlitsstjórnvalds.

[3] Formin nefnast: Frávik-fft og Frávik-lv fyrir fjármálafyrirtæki annars vegar og lífeyrissjóði og vátryggingafélög hins vegar.

Upphafstilkynning

Innan *fjögurra klukkustunda* frá því að atvik er flokkað sem stærra frávik skal fylla út rauða flipann í forminu og senda inn í gegnum gagnaskilakerfið.

Hér fyrir neðan er dæmi um útfyllingu frá banka um ímyndaða DDoS árás á hann:

Initial report	within 4 hours after classification of the incident as major

Report date *(DD/MM/YYYY)*	~~4.1.2021~~	Time *(HH:MM)*	~~13:40~~

A - Initial report					
A 1 - GENERAL DETAILS					
Type of report					
Type of report	Individual				
Affected Financial Institution (SE)					
SE name	Banki hf.f				
SE national identification number	333333-2020				
Head of group, if applicable					
Country / countries affected by the incident	AT BE BG CY CZ DE DK EE ES FI FR GB GR H R HU IE IS IT LT L U LV MT NL NO PL PT RO SE SI S K				
Primary contact person	Jón Jónsson	Email	jón@banki.is	Telephone	123 4567
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected SE in case of delegated reporting)					
Name of the reporting entity					
National identification number					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
A 2 - INCIDENT DETECTION and CLASSIFICATION					
Date and time of detection of the incident *(DD/MM/YYYY, HH:MM)*	~~04/01/2021, 6:20~~				
Date and time of classification of the incident *(DD/MM/YYYY, HH:MM)*					
The incident was detected by		If 'Other', please specify:			
Type of Incident					
Criteria triggering the major incident report	Imp. Services affected; FI users affected; Service downtime; Breach of security measures; Economic impact; High level of internal escalation; Other FIs or relevant infrastructures potentially affected; Reputational impact				
A short and general description of the incident	Stór DDoS árás sem varði í 4 klst og blokkeraði netbanka og app bankans				
Impact in other EU Member States, if applicable					
Reporting to other authorities	Yes	If 'Yes', please specify:	CERT-IS		

Fjármálaeftirlitið mun staðfesta móttöku tilkynningar og gefa tilkynningunni númer sem skrá skal í skjalið (í bláu og grænu flipana).

Framvinduskýrsla

Innan *þriggja vinnudaga* frá upphafstilkynningu skal senda inn framvinduskýrslu um atvikið. Fylla skal út bláa flipann í skjalinu og senda inn. Hér þarf að skrá nánari greiningu á atvikinu eftir bestu getu.

Major Incident Report

Intermediate report	maximum of 3 working days from the submission of the initial report	Reset dropdown selections

Report date *(DD/MM/YYYY)* | Time *(HH:MM)*
Incident reference code

B - Intermediate report

B 1 - GENERAL DETAILS

More detailed description of the incident:			
What is the specific issue?			
How did the incident start?			
How did it evolve?			
What are the consequences (in particular for payment service users)?			
Was the incident communicated to payment service users?		If 'Yes', please specify:	
Was it related to a previous incident/s?		If 'Yes', please specify:	
Were other service providers/third parties affected or involved?		If 'Yes', please specify:	
Was crisis management started (internal and/or external)?		If 'Yes', please specify:	
Date and time of beginning of the incident (if already identified) *(DD/MM/YYYY HH:MM)*			
Date and time when the incident was restored or is expected to be restored *(DD/MM/YYYY HH:MM)*			
Functional areas affected	☐ Authentication/Authorisation ☐ Direct settlement ☐ Communication ☐ Indirect settlement ☐ Clearing ☐ Other	If 'Other', please specify:	
Changes made to previous reports			

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Transactions affected [2]	Impact level		
	Number of transactions affected		
	As a % of regular number of transactions		
	Value of transactions affected in EUR		
	Duration of the incident (only applicable to operational incidents)		
	Comments:		
Payment service users affected [3]	Impact level		
	Number of payment service users affected		
	As a % of total payment service users		
Breach of security of network or information systems	Describe how the network or information systems have been affected		
Service downtime	Total service downtime:	Days: / Hours: / Minutes:	
Economic impact	Impact level		
	Direct costs in EUR		
	Indirect costs in EUR		
High level of internal escalation	Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	Describe how this incident could affect other PSPs and/or infrastructures		
Reputational impact	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of law...)		

B 3 - INCIDENT DESCRIPTION

Type of Incident			
Cause of incident	☐ Under investigation ☐ Malicious action ☐ Process failure ☐ System failure ☐ Human errors ☐ External events ☐ Other	If 'Other', please specify:	
Was the incident affecting you directly, or indirectly through a service provider?		If 'Indirectly', please provide the service provider's name:	

B 4 - INCIDENT IMPACT

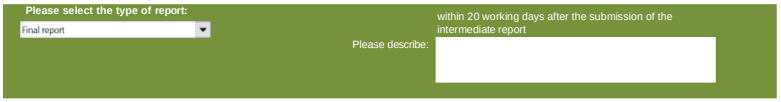
Overall impact	☐ Integrity ☐ Availability	☐ Confidentiality ☐ Authenticity	
Commercial channels affected	☐ Branches ☐ E-banking ☐ E-commerce	☐ Telephone banking ☐ Mobile banking ☐ ATMs	☐ Point of sale ☐ Other
	If 'Other', please specify:		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments	☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments	☐ Money remittance ☐ Payment initiation ☐ Account information services

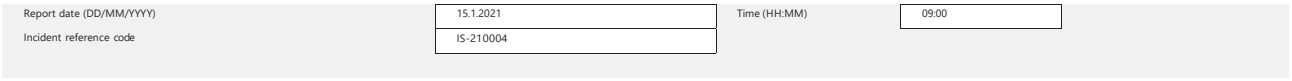
B 5 - INCIDENT MITIGATION

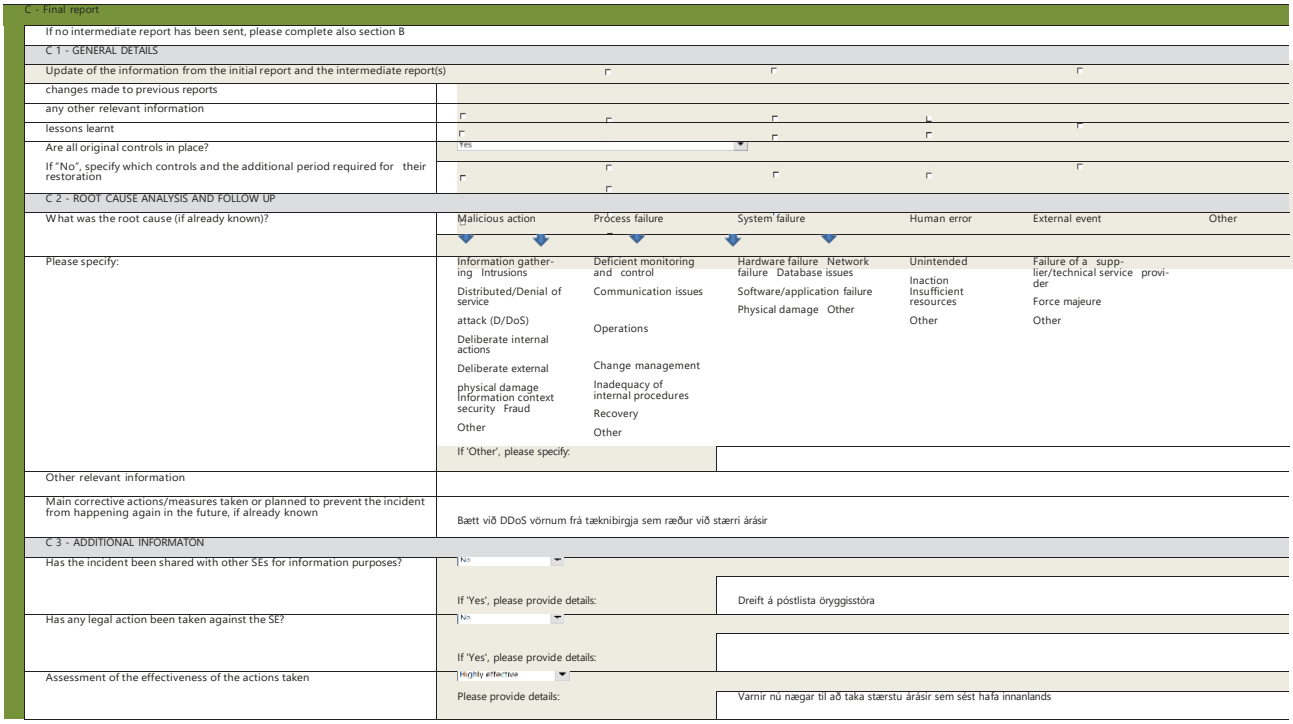
Which actions/measures have been taken so far or are planned to recover from the incident?	
Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?	
If so, when? *(DD/MM/YYYY HH:MM)*	
If so, please describe	

Lokaskýrsla

Lokaskýrslu um frávikið skal skila innan *20 vinnudaga* frá því að fráviki telst lokið. Fylla skal út græna flipann í skjalinu og senda inn.



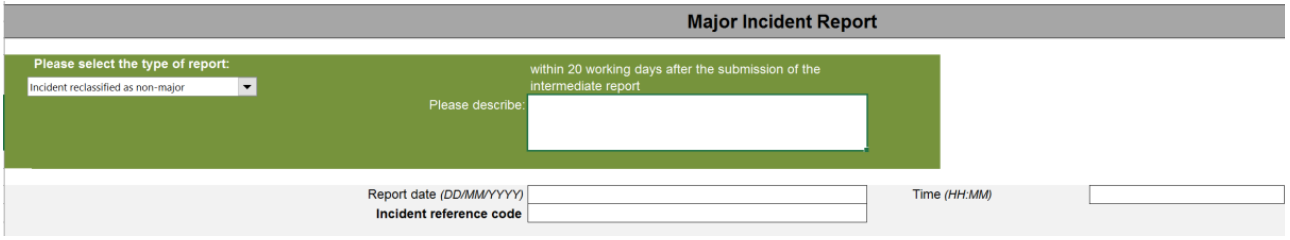




Endurskilgreining fráviks

Ef frávik hefur á einverjum tímapunkti innan 20 daga eftir upphafstilkynningu, verið endurflokkað sem ekki stærra frávik skal fylla út græna flipann og skila inn með merkingu um endurflokkun á fráviki með skýringu. Eftir það þarf ekki að skila frekari tilkynningum vegna fráviksins.

Ef frávik klárast hratt, má skila samtímis einni eða fleiri af ofangreindum skýrslum.



Sameiginlegar tilkynningar frávika

Heimilt er að veita tækniþjónustuveitendum umboð til að tilkynna beint til fjármálaeftirlitsins frávik sem verða hjá þjónustuveitanda og þarf þá eftirlitsskyldur aðili ekki að gera það. Gera þarf skriflegan samning um þetta á milli þjónustuveitanda og eftirlitsskylds aðila og tilkynna til fjármálaeftirlitsins.