# 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).

## Hvað skal tilkynna

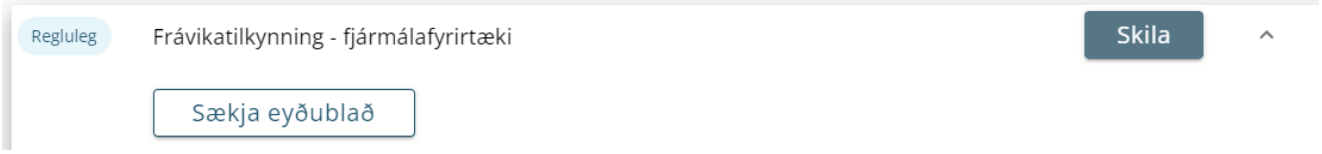
Tilkynna skal meiriháttar frávik samkvæmt viðmiðum í neðangreindri töflu. Tilkynna skal frávik ef þrjú eða fleiri atriði í dálknum „Lægra viðmið“ eiga við og/eða eitt atriði í dálknum „Hærra viðmið“:

| Skilyrði | Lægra viðmið | Hærra viðmið |
|---|---|---|
| Hlutfall mikilvægar þjónustu sem varð fyrir áhrifum | >10% af venjulegu umfangi þjónustu og lengd atviks > 1 klst **eða** > 15 m.kr (€500.000) og lengd atviks > 1 klst | >25% af venjulegu umfangi þjónustu **eða** > 400 m.kr (€15.000.000) |
| Fjöldi notenda sem urðu fyrir áhrifum | > 500 og lengd atviks > 1 klst **eða** > 10% af notendum mikilv. þjónustu og lengd atviks > 1 klst | > 5.000 eða > 25% af notendum mikilv. þjónustu |
| Niðritími þjónustu | > 2 klst | |
| Brot á öryggisráðstöfunum | Já | |
| Fjárhagsleg áhrif fráviks | | >Max (0.1% T1 fjármagn, 5 m.kr) eigið tap **eða** > 150 m.kr. |
| Stigmögnun viðbragða | Já | Já og líklegt að neyðaráætlun verði virkjuð |
| Áhrif á aðra EA eða mikilvæga innviði | Já | |
| Áhrif á orðspor | Já | |

## Framkvæmd

Meiriháttar frávik í rekstri eftirlitsskyldra aðila skal tilkynna til fjármálaeftirlitsins í gagnaskilakerfi Seðlabankans: https://gagnaskil.sedlabanki.is/

Þar er að finna frávikaskráningarform sem nota skal við tilkynningar.




Hvert meiriháttar 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:

Sí. 4.1.13.

## Upphafstilkynning

Innan *fjögurra klukkustunda* frá því að atvik er flokkað sem meiriháttar 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 ☐ DE ☐ FR ☐ IE LV ☐ PT<br>☐ BE ☐ DK ☐ GB ☑ IS ☐ MT ☐ RO<br>☐ BG ☐ EE ☐ GR ☐ IT ☐ NL ☐ SE<br>☐ CY ☐ ES ☐ HR ☐ LT ☐ NO ☐ SI<br>☐ CZ ☐ FI ☐ HU ☐ LU ☐ PL ☐ SK | | | | |
| Primary contact person | Jón Jónsson | Email | jon@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 | Internal organisation | If 'Other', please specify: | | | |
| Type of Incident | Security | | | | |
| 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.

| Intermediate report | maximum of 3 working days from the submission of the initial report |
|---|---|

Report date (DD/MM/YYYY) [illegible] Time (HH:MM) [illegible]
Incident reference code I5-230004

**B - Intermediate report**

**B 1 - GENERAL DETAILS**

| | | | |
|---|---|---|---|
| **More detailed description of the incident:** | | | |
| What is the specific issue? | Stór DDoS árás gerð erlendis frá. Netsamir höldu ekki allveg og netbanki og app duttu út. | | |
| How did the incident start? | Þegar árásin hófst. | | |
| How did it evolve? | Í byrjun hélda vamir en þegar stærð árásar óx, höldu þær ekki lengur. | | |
| What are the consequences (in particular for the institutions users)? | | | |
| Was it related to a previous incident? | No | If 'Yes', please specify: | |
| Were other service providers/third parties affected or involved? | Yes | If 'Yes', please specify: | Internetþjónustufyrirtæki |
| Was crisis management started (internal and/or external)? | No | If 'Yes', please specify: | |
| Date and time of beginning of the incident (if already identified) (DD/MM/YYYY, HH:MM) | [illegible] | | |
| Date and time when the incident was restored or is expected to be restored (DD/MM/YYYY, HH:MM) | [illegible] | | |
| Functional areas affected | ☐ Core banking services ☐ Foreign services ☒ Payment services ☐ Investment activities ☐ Insurance services ☐ Other | If 'Other', please specify: | |
| Changes made to previous reports | | | |

**B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT**

| | | | | |
|---|---|---|---|---|
| Important services affected [1] | Number of important services affected | 2 | Actual figure | |
| | % of regular important service affected (max) | 100% | Actual figure | |
| | Value of services affected in ISK | 1.000.000 | Estimation | |
| | Duration of the incident (only applicable to operational incidents) | >= 1 hour | Actual figure | |
| | Comments: | | | |
| Entities users affected [2] | Number of entities users affected | 20.000 | Actual figure | |
| | As a % of total institution users | 100% | Actual figure | |
| Breach of security measures | | | | |
| | Describe how the information security policy has been violated | | DDoS árás er alltaf brot á netöryggi | |
| Service downtime | >= 2 hours | | | |
| | Total service downtime (DD:HH:MM) | 00:04:10 | Actual figure | |
| Economic impact | Yes | | | |
| | Direct costs in ISK | 2.000.000 | Estimation | |
| | Indirect costs in ISK | 1.000.000 | Estimation | |
| High level of internal escalation | Yes, and crisis mode (or equivalent) is likely to be called upon | | | |
| | 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 | | Framkvæmdastjórn upplýst. Notvarnarhópar stofnur. | |
| Other SEs or relevant infrastructures potentially affected | No | | | |
| | Describe how this incident could affect other SEs and/or infrastructures | | | |
| Reputational impact | Yes | | | |
| | Describe how the incident could affect the reputation of the SE (e.g. media coverage, potential legal or regulatory infringement…) | | Niðritími á notendaþjónustu alltaf neikvæður | |

**B 3 - INCIDENT DESCRIPTION**

| | | | |
|---|---|---|---|
| Type of Incident | Security | | |
| Cause of incident | ☐ Under investigation ☒ Malicious actions ☐ 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? | Directly | If 'Indirectly', please provide the service provider's name: | |

**B 4 - INCIDENT IMPACT**

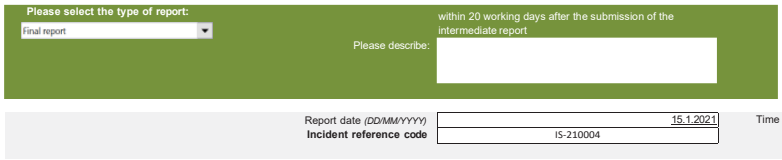
| | | | |
|---|---|---|---|
| Overall impact | ☐ Integrity ☒ Availability | ☐ Confidentiality ☐ Authenticity | |
| Commercial channels affected | ☐ Branches ☒ E-banking ☐ E-commerce | ☐ Telephone banking ☒ Mobile banking ☐ ATMs | ☐ Point of sale ☐ Other |
| | If 'Other', please specify: | | |
| Payment 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 ☐ Other |
| | If 'Other', please specify: | | |

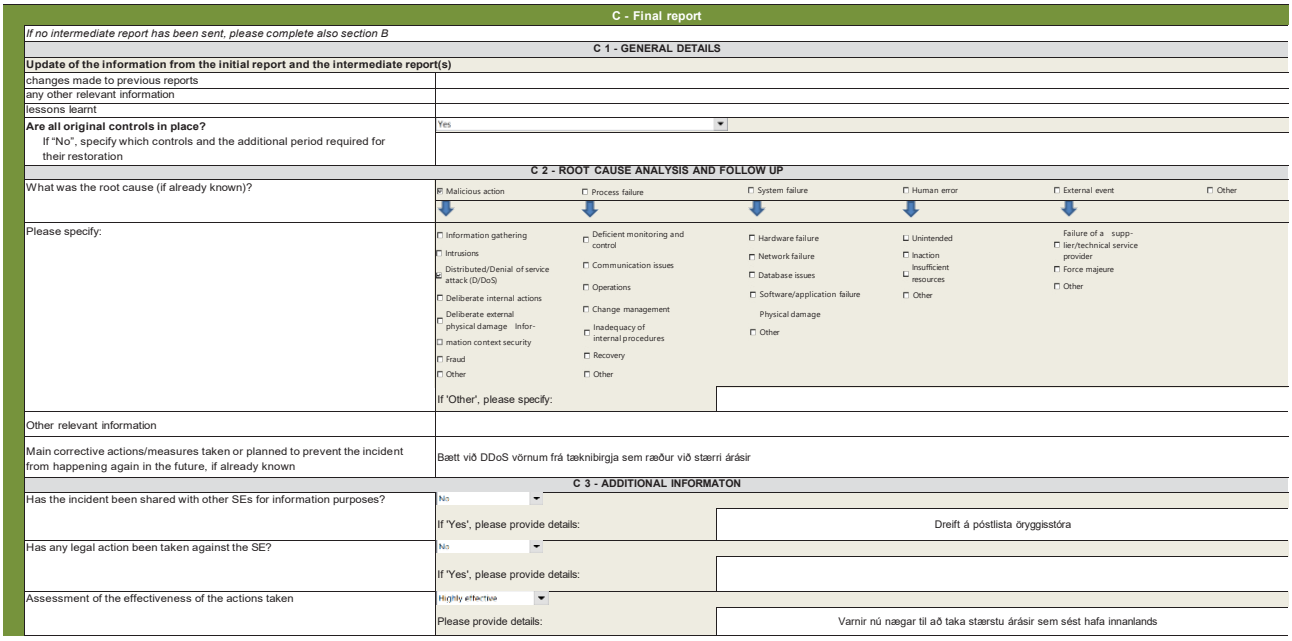
**B 5 - INCIDENT MITIGATION**

| | |
|---|---|
| Which actions/measures have been taken so far or are planned to recover from the incident? | Auknum DDoS vörnum bætt við frá tæknibirgja |
| Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? | No |
| If so, when? (DD/MM/YYYY, HH:MM) | |
| If so, please describe | |
| Has the SE cancelled or weaken some controls because of the incident? | No |
| If so, please explain | |

## 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.

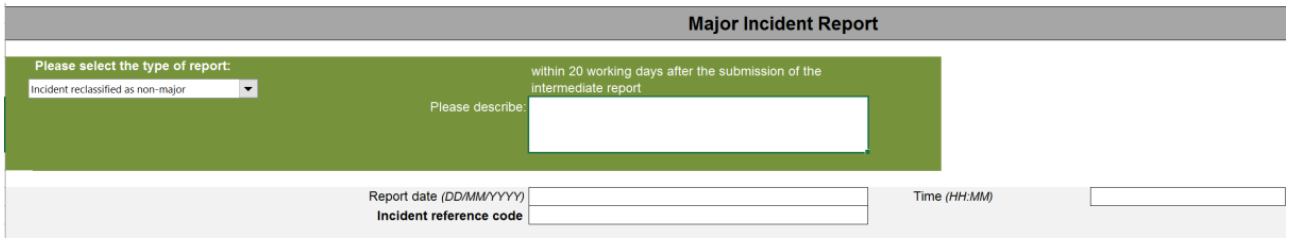



*Endurskilgreining fráviks*

Ef frávik hefur á einverjum tímapunkti innan 20 daga eftir upphafstilkynningu, verið endurflokkað sem ekki meiriháttar 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 fá sameiginlega þjónustuveitendur eins og Reiknistofu Bankanna (RB) eða tækniþjónustuveitendur 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. Samhliða þarf að fá aðgang fyrir viðkomandi þjónustuveitanda að þjónustuvefnum hjá fjármálaeftirlitinu.

Þjónustuveitandi getur tilkynnt frávik sem snerta fleiri en einn eftirlitsskyldan aðila í einu lagi, og þarf þá gefa upp hvaða eftirlitsskyldu aðila frávikið snertir (sjá töflu neðst í flipunum í skjalinu)[1].

[1] Þessi virkni er í þróun í gagnaskilakerfi Seðlabankans.