FIA.org

FIA Response to RTS and ITS on content, timelines and templates on incident reporting

Question 1. Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

- FIA and FIA EPTA ('The Associations') continue to support the EBA Guidelines for proposed timelines.

- The Associations note that the DORA incident reporting regime is more comprehensive and has shorter timelines than ECB, NIS2 and PSD2 incident reporting regimes and any equivalent jurisdiction. We strongly recommend the ESAs consider any attempts to reduce the reporting burden being placed on financial entities throughout all reporting stages.

- Data fields in the DORA reporting regime align most closely with PSD2 data fields. We note that DORA includes ICT systems and other financial services that do not all relate closely to specific criteria as is the case with payments incidents. Payment incidents immediately align to transactions figures, clients, geographic location and root causes whereas this information, alongside other fields such as economic cost, can be more difficult to determine if an incident relates to a financial entity's ICT applications. The Associations therefore request greater 'yes, if applicable' data fields for classification criteria and for the majority of information to be included in the final report only. Any attempts to determine incident impact information within the 72 hour intermediate deadline will impede incident risk management and detract financial entity attention from resolving and responding to an incident effectively.

- As for the content for each of the reports, The Associations recommend that the ESAs indicate that the specified content for each report should be provided "on a best effort basis". We therefore suggest that this is specified in each Article related to the content to be provided for the initial, intermediate, and final reports.

- Article 6(1)(a) – The timeline to send the initial report is not clear. We request the ESAs consider an alternative reporting trigger focused on the time an FE "becomes aware" of the incident. See below for suggested changes to timelines:

  a. Request to consider amending the initial notification timeline in Article 6 to read as follows: "*a) the initial report shall be submitted as soon as possible but not later than 24 hours after the FE has determined an incident has met the threshold of a major ICT incident*" – given information at this stage is limited, **the required data fields should be limited to what is available to the FE at the time of submission**. It is highly likely that FEs will have a good sense of whether the incident will meet the major ICT incident threshold. Allowing FEs to report prior to definitively confirming thresholds were met will prevent FEs from having to do detailed analysis at a critical time of the incident response and recovery process.

  Furthermore, for an incident to be classified as major, it needs to meet multiple criteria. It is possible for an incident to initially not breach those thresholds but in a span of 48 hours be classified as major. In such instances, it is not possible to adhere to the 24-hour window of the RTS.

The Associations urge the ESAs to consider that during the first 24 hours of an incident, FEs often must communicate with key internal stakeholders, work toward incident remediation, and document key decision points made throughout the incident management process. Additionally, if the incident is malicious, FEs have the added responsibility of coordinating enforcement procedures and determining several additional factors, including how the threat actor entered their network, the actions that occurred upon entry, the assessment against incident classification criteria, and finally, determining when it is safe to bring systems back online. Given the frequency and severity of cyber-attacks (particularly ransomware) on the financial services industry, it would be beneficial to promote an early warning notification with a limited reporting requirement to alert competent authorities of necessary information about the major incident that would enable authorities to potentially identify emergent risks that may challenge operations of the financial services industry without unduly burdening FEs with detailed reporting requirements.

As a result, the Associations request the ESAs consider including only the most pertinent information on an initial report, to be provided on a best effort basis given information related to incidents is fluid in its early stages and allow for response teams to focus more resources on recovery efforts. The Associations view the following elements as appropriate for the initial report:

a) Date and time of detection and classification of the incident;
b) Description of the incident;
c) Classification criteria that triggered the incident report in accordance with [Articles 1 to 8 of Delegated Regulation [insert number once published in official journal]
(j) Other information

As a result, the Associations request that the ESAs consider moving Article 3(d-i) out of the initial report and into the intermediate report. The Associations view the information expected in Article 3(d-i) to be more appropriate for the intermediate report, rather than the initial report, for reasons described above.

b. Subsequently, the intermediate report timeline should be amended to read “an intermediate report shall be submitted as soon as possible but not later than 72 hours after regular activities have been recovered and business is back to normal; if regular activities have not yet been recovered, financial entities shall submit the intermediate report within 72 hours from the submission of the initial report”. This report should include an option for the financial entity to confirm that the incident met the major ICT incident threshold therefore, data fields 2.4 and 2.5 in Annex II should be moved to the intermediate report rather than the initial report.

c. To be consistent with the above recommendations, we would request the final report timeline to be “the final report shall be submitted as soon as possible but not later than one month from when business is back to normal.”

- It is important to note that the alignment of timelines for incident reporting to match those stipulated in NIS i.e. 4h/24h for the initial notification, 72 hours for the intermediate report **involves a decrease of time limits for all incidents which are currently reported under PSD2**. In PSD2, the suggested initial report submission timelines refer to business hours. Meeting the timelines proposed in this RTS, which include non-business

hours, might be difficult – especially if an incident occurs out of business hours. Even though Article 4 specifically allows extensions for the set time limits, we would like to point out that the tight time limits might lead to an increased reporting / communication effort.

- **Weekend and bank holiday reporting**:

  Article 6(2) should allow flexibility also for the initial report. Furthermore, reporting within one hour of the next working day is not practicable for smaller organisations and we suggest amending Article 6(2) as follows:

  "Where the deadline for submission of an **initial**, intermediate report or a final report falls on a weekend day or a bank holiday in the Member State of the reporting financial entity, financial entities may submit the **initial**, intermediate or final reports ~~within one hour~~ **as soon as possible** following regular starting time of the next working day and **in all cases no later than the end of the next working day."**

  Furthermore, the industry notes in 6(3) that the flexibility concerning the reporting of incidents in a weekend or bank holiday of the Member State of the reporting financial entity is not applied to significant credit institutions, where the incident affects another Member State or if the entity is systemic according to the competent authority by the national market. We believe further flexibility should be allowed for all financial institutions in relation to the submission of intermediate or final reports, especially if an incident relates to another Member State. Incidents can relate to ICT systems, or other Member State activities, that are not systemic in nature and do not reflect an essential service or commercial impact to clients and the operations of the financial entity. **The ability to procure information during a weekend or bank holiday can reduce the level of information included within reporting and it does not relate to the ability of the financial entity to respond and manage an incident.** We do not believe that the intermediate or final reports are required during this period and to what extent that information is required by the authority.

- **The economic costs and losses templates should align more clearly within the incident classification criteria**. The instructions and descriptions within the costs and losses criteria (4.13-4.25) could infer that a financial entity would have to provide economic cost information that could relate to normal business activity. As stated in the classification criteria and aggregated cost and losses guidelines, losses only relate to costs "exceeding business-as-usual costs" or "are necessary to run the business as usual." The templates, especially in relation to staff costs, could easily reach the criteria for major reporting and be inconsistent with the stated classification criteria. A further recital or amendments to specific fields could create more certainty for financial entities:

  - NEW <u>(5) The economic impact of the incident shall be based on Article 7 of the proposed RTS under Article 18(3) DORA and only include costs and losses that exceed the business-as-usual costs.</u>
  - 4.17 staff costs: "amount of staff <u>costs that exceed business-as-usual costs</u>, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff"

- **Time zone**: Further clarification is required regarding the time zone that the financial entity should utilize for incident reporting. It is unclear if this should be based on the reporting financial entity, the Member State that is receiving the report or the location of the incident.

Question 2. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

- FIA welcomes additional clarification of the reporting obligations for subsidiaries of financial entities and would like to seek clarity about the reporting channels and obligations for ICT incidents that affect global systems in a global group:

  - e.g. What are the reporting obligations concerning an ICT incident in a global ICT system that is classified as a major incident for a subsidiary but not at group level ?

- Article 2(c) – FIA recommends removing the requirement to include contact details of the contact person responsible for communicating with the competent authority – FEs should be permitted to use a shared mailbox or somebody who isn't an individual given the fluid nature of incidents and to avoid being overly reliant on one individual.

- 2.6 Discovery of the incident: The criteria chosen by the ESAs concerning how the incident has been discovered are undefined and could be interchangeable. For instance, an 'IT Security' incident could relate to production management whereas 'Staff' could also relate to all criteria. We would welcome the reintroduction of PSD2 categories 'Detected Internal' and 'Detected External' to show how financial entities normally discover incidents in practice.

- 2.8, 2.9 and 2.10 Description of the incident: We recommend that data fields 2.8 – 2.10 are combined to one, single data field. Note that financial entities are likely unable to come to an accurate determination of the impact of incidents to other financial entities and third party providers in all circumstances. Financial entities are highly unlikely to know the impact by the initial notification timelines and we recommend this requirement should be switched to 'Yes, if applicable' at this stage. As incidents rarely affect other financial entities or third party providers, we recommend that data field 2.8 is changed to 'Yes, if applicable' in all reporting stages.

- 2.11 Information whether the major incident has been recurring: It is unclear why 2.11 is mandatory for all report stages. If a major incident is determined as major due to it recurring, then financial entities will report on that basis under 'Yes, if applicable'. We recommend the inclusion of this data field is switched to 'Yes, if applicable' across all reporting stages.

Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

- 3.3 Date and time of occurrence of the incident: It is unclear how this data field relates to recurring incidents and we welcome further clarification. The Associations seek clarification on whether recurring incidents only

need to be reported as part of the monthly review when a recurring incident reaches the threshold of a major incident, and not at the time a FE deems a recurring incident to reach a threshold of a major incident.

- 3.6 Number of clients affected: Clients are not always affected by an incident and we recommend that this data field is switched from mandatory to 'yes, if applicable' in the intermediate and final reporting stage. We recognise that this field is mandatory within PSD2, however, PSD2 relates to payment transactions which have a logical attachment to clients being affected by incidents. DORA's incident reporting places in-scope a wider set of incidents, including internal system-based incidents, which do not always affect clients.

- 3.7 Percentage of clients affected: As per above, DORA applies to a wide range of incidents that do not always relate to clients. We believe all reporting stages should be 'yes, if applicable'.

- 3.15 – 3.16 Reputational impact: The criteria and contextual information included within the reputational reporting criteria are onerous and do not relate to the ability of the financial entity to respond to the incident. The information infers that the financial entity should be undertaking significant research of local newspapers, blogs and social media platforms at all stages of responding to an incident, which would detract the financial entity from responding effectively to the incident at hand. We recommend that a determination for 'reputational impact' should be based on the national newspapers of the relevant Member State where the incident has taken place and/or financial news of note.

- 3.30 – 3.31 Affected infrastructure data fields: Financial entities are only fully aware of the impact and location of an internal ICT-system incident once the root cause of the incident has been reached. On that basis, we encourage that the data field is only mandatory in the final reporting stage as per the period when root cause is reported. If the financial entity is aware of the exact location of the infrastructure incident, then the financial entity is aware of the root cause of the incident. A financial entity would only be able to respond to 3.31 at the final stage of reporting.

- 3.35 Temporary actions/ measures taken: We recommend that the data field concerning temporary actions and the 3.37 field describing those actions should only be required in the final reporting stage. By the intermediate stage, the financial entity should be concentrating on responding to the incident and determining the most effective response. Actions will likely change materially through the reporting process and the intermediate stage will likely provide inaccurate information or out-of-date information. We recommend the reporting stage for intermediate is 'no' and the final reporting stage is 'yes, if applicable' reflecting instances whereby the incident did not require action on behalf of the financial entity (i.e. external events without an impact). In addition, the field choice of 'yes' in 3.36 does not relate effectively to the level of descriptions included within 3.38 (i.e. Disaster Recovery site activated). The descriptions in 3.38 infer a severe incident that is rare and we therefore suggest 3.37 should be a field for temporary actions taken in relation to a severe incident scenario.

- 3.38 – 3.39 Information on involvement of CSIRTs: It is unclear how the reporting authority will use the information in this data field. A financial entity is unlikely to itemize the actions of a CSIRT during an incident response and is unclear why a financial entity should be reporting on the behaviour of another Member State authority via an incident report. We suggest this data field is removed.

- 3.40 Indicators of compromise: A financial entity will be unaware of this information by the intermediate stage of reporting and we suggest the data field is change to 'No'. The field should not be mandatory if 'cybersecurity' is chosen within 3.26 for the intermediate report as a financial entity will not have the level of information to report reliably, at this level of detail, at that reporting stage. The information requested is highly burdensome and will detract a financial entity from responding to the incident.

- 3.41 Vulnerabilities exploited: The reporting of specific vulnerabilities can include confidential information that represents a significant cybersecurity risk to financial institutions. Given the risk being placed on the financial entity, including examples of how to expose vulnerabilities within a financial entity, it is unlikely a financial entity will provide any sensitive information in the 3.41 data field. We recommend the field is removed or any information provided will likely be of limited use to the reporting authority.

Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

- 4.1 Information about the root causes of the incident: According to the Final Report for incident classification, the data field 4.1 provides the list of root causes that financial entities will be required to use to determine whether a recurring incident has occurred. The list included in 4.1 correctly provides high-level root cause information but it does not provide the specificity or logic that can be used to determine if an incident has recurred. A significant majority of incidents will be based on two root causes included (2.d.ii; 3.d) relating to change management and software compatibility. An incident relating to change management or software compatibility can relate to a multitude of different factors and their repetition across incidents can have no relevance to each other. The data fields included in 4.1 are therefore too high-level and too diffuse to correctly attribute and compare across incidents, as the very nature of incidents is highly specific and does not necessarily always correlate with each other clearly. A financial entity needs a greater level of flexibility to determine what a repeating root cause is across incidents in order to not report irrelevant incidents or confuse authorities. The stated intention of the recurring classification is to demonstrate where there are "significant deficiencies and weaknesses in the financial entity's incident and risk management procedures." Unrelated root cause similarities will result in arbitrary reporting that has limited to no relevance to a financial entity's incident and risk management procedures and could result in regulatory supervision unintentionally focusing on deficiencies in the financial entity that do not exist.

We propose the following amendments to 4.1 and 4.3:

  - 4.1 Root causes of the incident; Instructions: "The following categories shall be considered <u>unless being reported as a reoccurring incident:</u>"
  - 4.3 Information about the root causes of the incident; Description: "Description of the sequence of the events that led to the incident <u>and description of root cause similarity when being reported as a recurring incident</u>."

  - 4.3 Information about the root causes of the incident; Instructions: "Description of the sequence of events that led to the incident including a concise description of all underlying reasons and primary

FIA.org

factors that contributed to the occurrence of the incidents. Include description of how the incident has a similar apparent root cause if the incident is classified as a recurring incident. The data field is mandatory if the incident is classified as a recurring incident."

- 4.4 Information about inability to comply with legal requirements: Incident reporting constitutes publicly reporting to unknown individuals within a financial entity's regulator and/or supervisor that could encompass a number of Member States. A financial entity will not be comfortable providing information, or hypothesising about, their inability to comply with legal requirements as this would introduce material legal exposure to the financial entity. There are material consequences to disclosing this information that could be irrelevant as the incident develops. An exercise of identifying all relevant regulations and their potential for non-compliance across all relevant Articles does not meaningfully contribute to common risk management practices or the resolution of the incident and the entity's services. We recommend that this data field is removed..

- 4.5 Information about breach of contractual arrangements/ SLAs: It is unclear regarding how the information in the data field will be utilised by authorities and how the information correlates to the incident and its impact. Contractual arrangements and SLAs are confidential and include client information that a financial entity will be uncomfortable in disclosing. As a financial entity will have to list client and financial counterparts within reports (3.6-3.10) and the costs of non-compliance (4.18), there is a risk that descriptions of contractual arrangements or SLAs could be linked to specific clients of the financial entity. This could place legal risk on the financial entity if costs were able to be linked directly to a client. As the data field does not relate to the incident and could reflect confidential information, we recommend this data field is removed.

- 4.8 Date and time when the incident was resolved and root cause addressed: The date and time when the incident was resolved is distinct from the date and time when the root cause is addressed. We recommend this data field is split into two data fields.

- 4.10 Information relevant for resolution authorities: The criteria included that would require the financial entity to contact the resolution authority are extreme incident scenarios which would likely results in a material interaction of supranational and national supervision teams engaging directly with the financial entity through the incident. It is highly unlikely for this extreme scenario to occur (ie one that impacts an entity's capital stack) and we recommend the field is removed or changed to 'yes, if applicable' in the final reporting stage.

- 4.14 – 4.23 Amount of costs: The level of information required for all data fields is highly onerous and would place a significant reporting burden on financial institutions to analyse incidents that could be vary significantly in scale. It is unclear concerning how this information would be used and why certain specific costs needs to be collected by authorities. The procurement of legal counselling, for instance, has limited relevance to incident response management and it is difficult to foresee how this information would be utilised by authorities. We recommend the cost analysis requirement are reduced significantly or changed to one data field-only. All examples in 4.23 are highly specific and do not appear to relate to incident management.

- 4.18 Amount of fees due to non-compliance with contractual obligations: Contractual information is confidential and there remains legal exposure and risk that information concerning clients affected by an incident could be attributed to fees due to non-compliance. In addition, non-compliance related cost is not charged nor determined within the 20 days period for a submission of a final incident report. As this field relates to confidential information, does not have relevance to the resolution of an incident and will likely be unavailable information, we recommend this field is removed.

Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.
N/A

Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.
N/A