Public Hearing on the Draft EBA Guidelines on Major Incidents Reporting under Article 96 of PSD2

Dirk Haubrich, Sergio Gorjón
Consumer Protection, Financial Innovation and Payments, EBA

Public Hearing, EBA, London, 9 February 2017

Agenda

1. **Introduction to the EBA**
   - The creation of the EBA and its scope of action
   - Legal instruments and output to date
   - Mandates conferred on the EBA under the PSD2
   - The purpose of public hearings
2. **The PSD2 mandate on the EBA for the Guidelines and the EBA's development approach**
   - The wording of the EBA mandate in the PSD2
   - Major incident reporting practices in Europe
3. **Draft Guidelines as proposed in the CP**
   - Structure of the Guidelines
   - Subject matter, scope and definitions
   - Guidelines addressed to PSPs (Guidelines 1-4)
   - Guidelines addressed to CAs (Guidelines 5-6)
   - Guidelines addressed to CAs (Guidelines 7-8)
4. **Next steps**

Introduction to the EBA

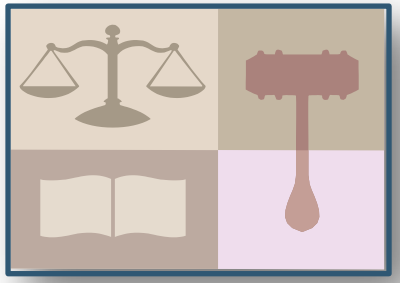
The creation of the EBA

- The EBA was established by Regulation (EC) No. 1093/2010 of the European Parliament and EU Council;
- came into being on 1 January 2011;
- took over all existing tasks and responsibilities from the Committee of European Banking Supervisors (CEBS);
- took on additional tasks, incl. consumer protection, the monitoring of financial innovation, and payments;
- is an independent authority;
- is accountable to the EU Parliament and Council;
- has as its highest governing body the EBA Board of Supervisors, comprising the Heads of the 28 national supervisory authorities.

Legal instruments available to the EBA

The EBA has different types of legal instruments at its disposal that differ in terms of purpose, legal status, and possible addressees.

- Technical standards
- Guidelines and recommendations
- Opinions / Technical Advice
- Warnings
- Temporary prohibitions
- Joint Positions
- Breach of Union law investigations
- Binding and non-binding mediation



The EBA's scope of action

The EBA's regulatory remit is defined by the EU Directives and Regulations that fall into its 'scope of action', either because they are listed in the EBA's founding regulation or because they confer tasks on the EBA. They include:

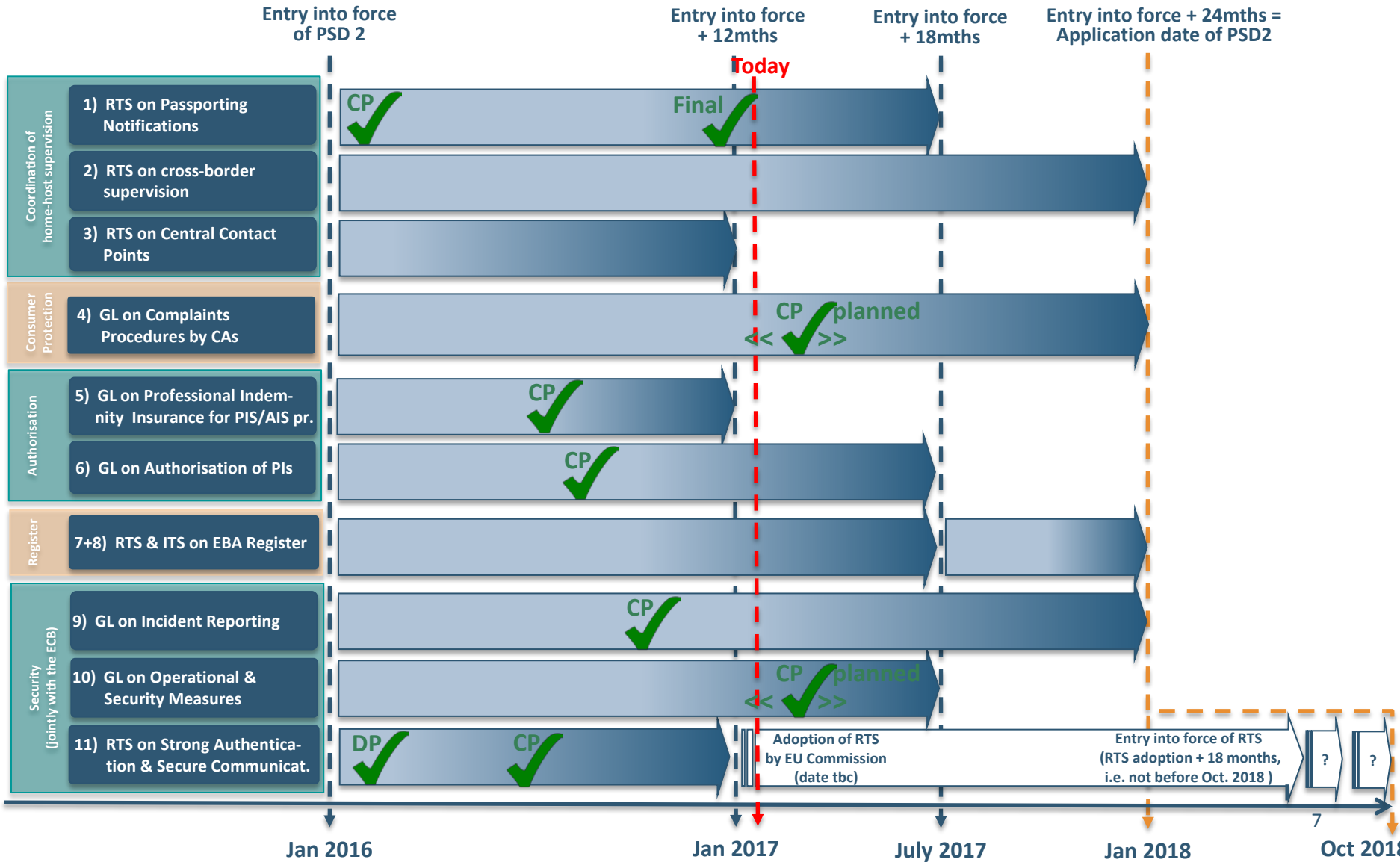
- Capital Requirements Directive (CRR/D IV)
- Deposit Guarantee Scheme Directive (DGSD)
- Mortgage Credit Directive (MCD)
- Payment Accounts Directive (PAD)
- Electronic Money Directive (EMD)
- Payment Services Directive (PSD1 + forthcoming PSD2)
- Anti–Money Laundering Directive (AMLD)
- Markets in Financial Instruments Directive (MiFID/R, for structured deposits)

Output of the EBA to date

Since its creation in 2011, the EBA has issued more than 200 legal instruments, as well as more than 100 reports.

	2011	2012	2013	2014	2015	Total
Regulatory Technical Standards	0	1	39	22	15	**77**
Implementing Technical Standards	0	0	21	10	9	**40**
Guidelines	2	6	2	17	19	**46**
Opinions / Technical Advice	1	6	6	14	21	**48**
Published reports	6	12	26	23	34	**111**
Recommendations	2	0	4	1	2	**9**
Breach of Union Law investigations	0	0	0	1	0	**1**
Mediations	0	2	5	0	0	**7**
Peer reviews	0	0	1	1	1	**3**
Warnings	0	0	2	0	0	**2**
Stress tests	1	0	0	1	1	**3**

Progress of EBA mandates under PSD2



The purpose of EBA public hearings

For many of its Technical Standards and Guidelines the EBA organises 'public hearings, with a view to allow interested parties to ask clarification questions.

- **An EBA hearing takes place during the consultation period, usually a month or so before the submission deadline of responses to the Consultation Paper (CP).**

- **The purpose of the hearing is for the EBA to present a summary of the CP, re-produce the questions of the CP, and asks attendees whether they require additional explanations or clarifications from the EBA so as to be able to answer the questions in the CP.**

- **The public hearing does therefore not replace written responses to the CP, as it is only through written responses that the EBA is able to give the views of stakeholders the required consideration.**

The PSD2 mandate on the EBA for the Guidelines and the EBA's development approach

The wording of the EBA mandate in the PSD2

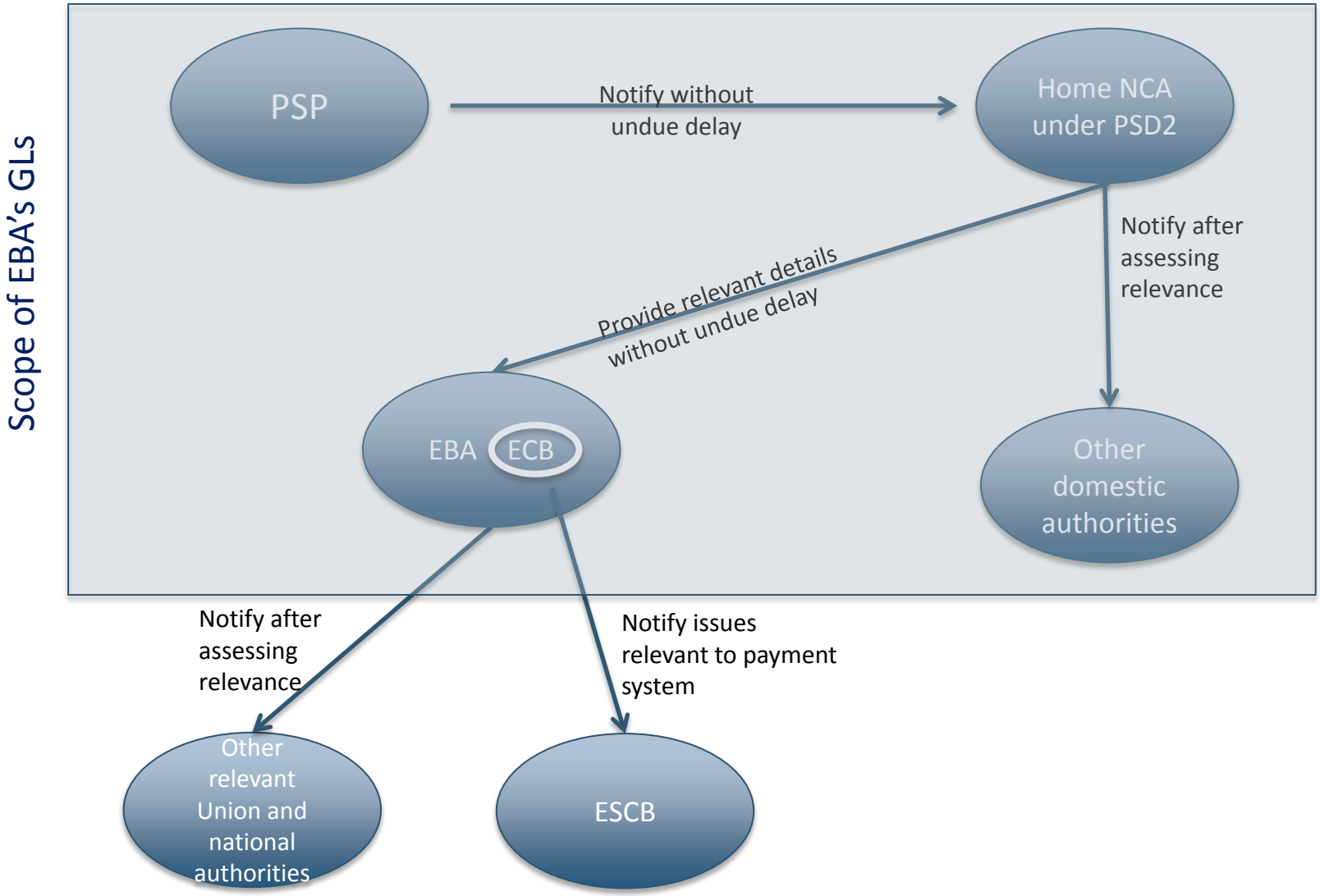
Article 96(3) of PSD2 confers on the EBA the following mandate:

"By 13 January 2018, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 addressed to each of the following:

(a) payment service providers, on the classification of major incidents referred to in paragraph 1, and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;

(b) competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities."

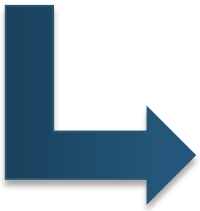
Article 96 of PSD2: Steps to be taken in case of a major operational or security incident



Major incident reporting practices in Europe

On account of the vast amount of experience on incident reporting across jurisdictions and authorities in the Union, before drafting the GLs the EBA set out to understand the strengths and shortcomings of these frameworks:

- Standards and/or specifications developed and published by the European Union Agency for Network and Information Security (ENISA)
- ECB SSM's pilot exercise on cyber-incident reporting
- Current incident reporting practices across supervisors and overseers



- *Clarity so as to facilitate practical implementation*
- *Comprehensiveness (range of incidents covered)*
- *Simplicity in acknowledgment of the diversity of PSPs*
- *Balanced approach (manageable compliance burden)*

Draft Guidelines proposed in the CP

Structure of the Guidelines

Given the wording of the mandate in Article 96(3), the EBA arrived at the view that the Guidelines should be structured into three separate sets.

Article 96 (3.a) mandates the EBA to develop Guidelines addressed to payment service providers, on the classification of major incidents and on the content, the format, including standard notification templates, and the procedures for notifying such incidents.

→ 1st set of Guidelines addressed to PSPs (Guidelines 1-4)

Article 96(3.b) mandates the EBA to develop Guidelines addressed to competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities.

→ 2nd set of Guidelines addressed to NCAs (Guidelines 5-6)

Article 96 (2) mandates the competent authority of the home Member State to provide, without undue delay, the relevant details of the incident to EBA and to the ECB.

→ 3rd set of Guidelines addressed to NCAs (Guidelines 7-8)

Subject matter, scope and definitions

- Operational or security incidents (actual or potential) with a material adverse effect on payment services in a broad sense: i.e.
  - Any of the business activities in the meaning of Article 4(3) of the PSD2
  - Any of the necessary technical supporting tasks for the correct provision of payment services
- "Material adverse effect" = "Major"
  - A major operational or security incident is a singular event or a series of linked events which have or may have a material adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services
- Payment services provided in the Union including where the major operational or security incident originates outside the Union and affects, either directly or indirectly, the payment services provided by a payment service provider located in the Union

Subject matter, scope and definitions

Consultation Questions

Q1: Do you consider the definitions included in the draft Guidelines to be sufficiently clear?

Guidelines addressed to PSPs (Guidelines 1-4)

Guideline 1: Incident classification: criteria

- Quantitative and qualitative criteria are used to classify incidents
- The degree of materiality results from establishing the nature of their impact as well as its scale
- The choice of criteria takes into account several aspects:
    - the degree to which potentially compromised dimensions are captured
    - the extent to which the notion of operational/security disruptions is reflected
    - their potential to allow for a quick and easy assessment (timeliness, accuracy, access)
    - their pre-existing level of implementation across markets
    - the feasibility of having them standardised and automated

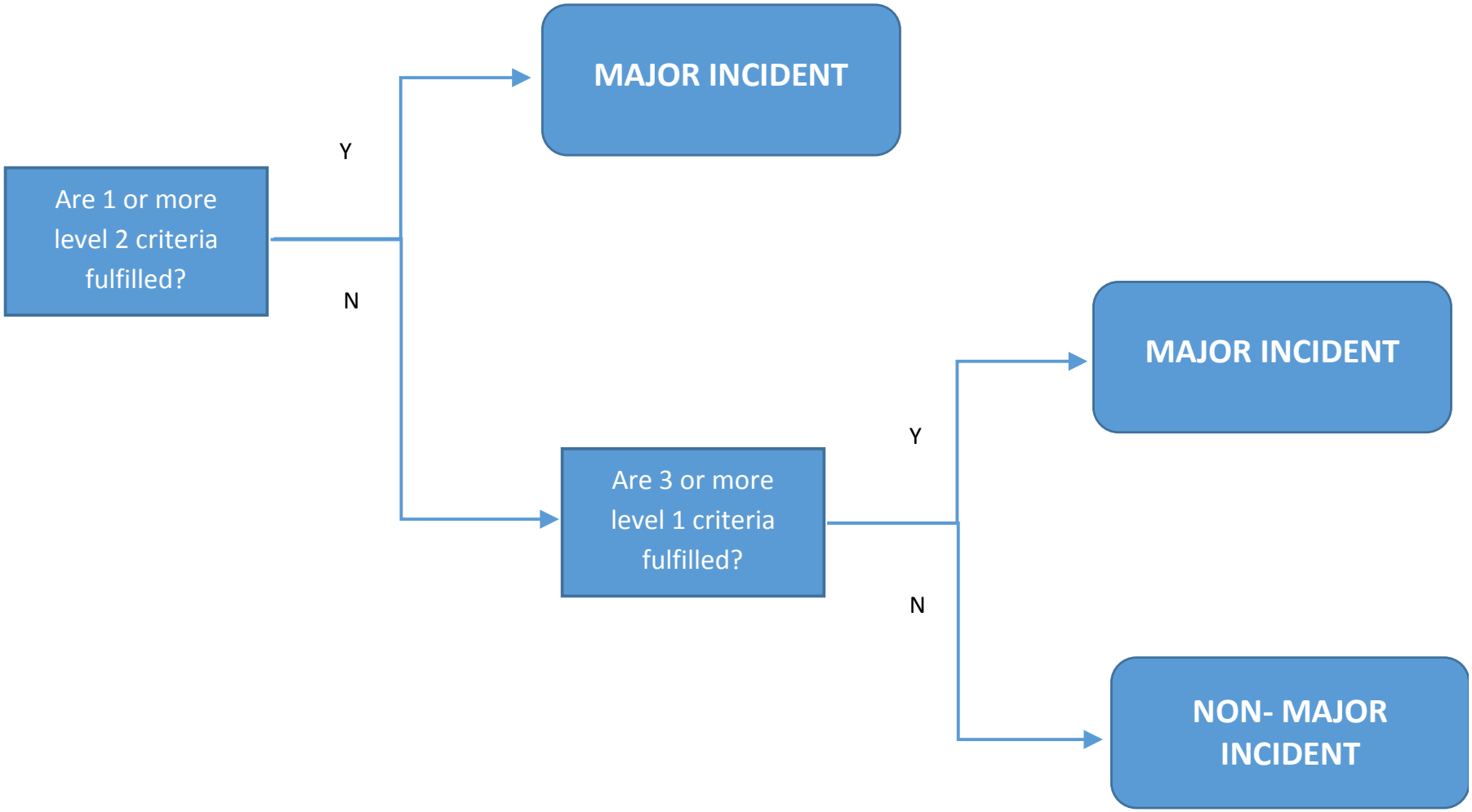
Guideline 1: Incident classification: criteria

Quantitative	Qualitative
Transactions affected	High level of internal escalation (outside regular reporting procedures)
Clients affected	Reputational impact
Service downtime	Potential to affect other payment service providers or relevant infrastructures
Economic impact	

Guideline 1: Incident Classification: thresholds

Criteria	Level 1	Level 2
Transactions affected	> 10 % of the payment service provider's regular level of transactions and > EUR 100,000	> 25 % of the payment service provider's regular level of transactions or > EUR 1,000,000
Clients affected	> 5,000 and > 10 % of the payment service provider's clients	> 50,000 or > 25 % of the payment service provider's clients
Service downtime	> 2 hours	-
Economic impact	-	> Max (0,1 % Tier-1 capital, EUR 200,000) or > EUR 5,000,000
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) was called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	-
Reputational impact	Yes	-

Guideline 1: Incident Classification: decision tree



Guideline 1: Incident Classification

Consultation Questions

Q2: Do you consider the criteria and methodology applicable for the assessment and classification of an incident as major to be sufficiently clear? If not, what should be further clarified?

Q3: Do you consider that the methodology will capture all of/ more than/ less than those incidents that are currently considered major? Please explain your reasoning.

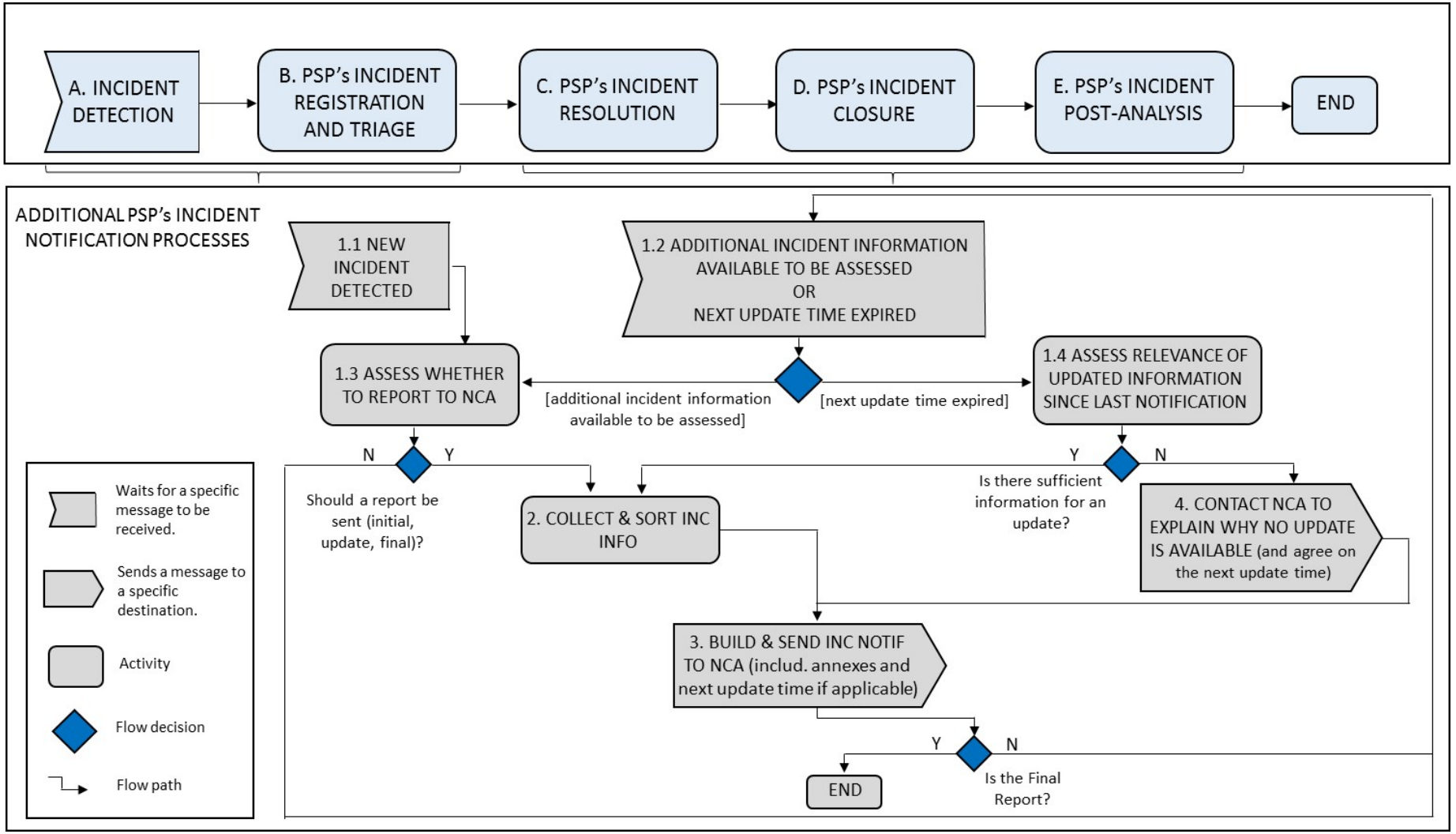
Q4: In particular, do you propose to add, amend and/or remove any of the thresholds referred to in Guideline 1.3? If so, please explain your reasoning.

Guideline 2: Notification process

- Single standardised template to be completed in an incremental manner throughout the life cycle of the incident
- Structured in eight sections: (1) general details, (2) incident discovery, (3) incident classification, (4) incident description, (5) incident impact, (6) incident mitigation, (7) root cause analysis and follow-up, and (8) additional information
- Additional explanatory documents can be voluntarily provided: e.g. internal incident reports, records of a third-party technical provider, statistics, etc.
- Three distinctive types of report: (i) initial, (ii) intermediate/delta, and (iii) final

Guideline 2: Notification process

Workflow



Guideline 2: Notification process

Consultation Questions

Q5: Do you think that the information depicted in the template in Annex 1 is sufficient to provide CAs in the home Member State with a suitable picture of the incident? If not, which changes would you introduce? Please explain your reasoning.

Q6: Are the instructions provided along with the template sufficiently clear and helpful to remove any doubts that could arise when completing the required fields? If not, please explain your reasoning.

Q7: As a general rule, do you consider the deadlines and circumstances that should trigger the submission of each type of report (i.e. initial, intermediate and final) feasible? If not, please provide a reasoning and justify any alternative proposal.

Guideline 3: Delegated and consolidated reporting

- Voluntary recourse to a third party for the completion of a PSP's reporting obligations

- Delegation = outsourcing of administrative tasks associated with the assessment, classification and submission of incident reports
  - Potential benefits include improved efficiency and quality of the reports
  - PSPs remain fully responsible and accountable
  - Requires a formal contract (allocation of responsibilities, safeguarding of the confidentiality, consistency, integrity and reliability of information)

- Consolidation = one single report which covers several PSPs at once
  - Typically when a common technical service provider is used
  - Limited to PSPs established in the same Member State
  - Where effects are dissimilar, differences need to be clearly spelled out

Guideline 3: Delegated and consolidated reporting

Consultation Questions

Q8: Do you consider that the delegated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

Q9: Do you consider that the consolidated reporting procedure proposed in the draft Guidelines will provide added value to the market? Please explain your reasoning.

Guideline 4: Operational and Security Policy

- General operational and security policies need to define clearly all the responsibilities and processes to ensure compliance with the requirements on incident reporting set forth in the GLs
- No additional organisational rules/communication requirements are foreseen on account of the diversity of PSPs and the need to accommodate national specificities

Guidelines addressed to CAs (Guidelines 5-6)

Guideline 5: Assessment of the relevance of the incident

- Differences in the legal frameworks/contractual arrangements call for a prioritisation of NCA's expert opinion
- Some primary indicators of the importance of an incident are provided yet NCAs can consider others as well
    - the cause of the incident is within the regulatory remit of another domestic authority
    - the consequences of the incident have an impact on the objectives of another domestic authority
    - incidents affect or could affect payment service users at a wide scale
    - incidents are likely to receive or have received wide media coverage
- Continuous assessment

Guideline 6: Information to be shared

- As a minimum, non-sensitive data elements should be shared with other domestic authorities at the time of receiving the initial report and the last intermediate report
  - Date of beginning and/or detection of the incident
  - Estimated or actual date of recovery
  - Short description of the incident (including non-sensitive parts of the detailed description)
  - Short description of measures taken or planned to be taken to recover from the incident
  - Description of how the incident could affect other PSPs and/or infrastructures
  - Description (if any) of the media coverage
  - Other impact (if relevant)
  - Cause of incident (including root cause, if already known)
- Proper anonymisation prior to circulating information
- Adequate measures to ensure confidentiality, integrity of data and authentication of the parties

Guidelines addressed to CAs (Guidelines 7-8)

Guideline 7: Information to be shared

- Maximalist approach: competent authorities should always provide EBA/ECB with all reports received from (or on behalf of) PSPs affected by a major operational or security incident: i.e.
    - Initial
    - Intermediate/delta
    - Final
- Other documents may be circulated as well
- Competent authorities should forward the report to EBA/ECB following the deadlines and procedures established by the latter

Guideline 8: Communication

- Competent authorities should at all times preserve the confidentiality and integrity of the information exchanged and their proper authentication towards EBA/ECB

- In order to avoid delays in the transmission of incident-related information to EBA/ECB and help minimise the risks of operational disruptions, competent authorities should report appropriate means of communication

Next steps

Next steps

- **7 March 2017:** Consultation period ends;
- **March - Jun2017:** EBA assesses CP responses to decide which, if any, changes will be made to the Guidelines before finalisation;
- **Summer 2017:** EBA will publish the Final Guidelines, in English language. The Guidelines will be part of a 'Final Report', which will also contain a 'feedback table' that lists all points made by respondents, and the EBA's assessment of whether changes were required;
- **Summer 2017:** EBA will publish the translations in all official EU languages. National authorities will then have two months to submit to the EBA compliance notifications stating whether or not they comply
- **13 January 2018:** Guidelines apply