SWIFT Response to the European Banking Authority on the Consultation Paper:

"Guidelines on major incidents reporting under the Payment Services Directive 2"

7 March 2017

SWIFT thanks the European Banking Authority for the opportunity to provide comments on the Consultation Paper 'Guidelines on major incidents reporting under the Payment Services Directive 2'.

SWIFT is a member-owned, cooperative society headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholding Users, comprising over 3,000 financial institutions. We connect more than 11,000 connected firms, in more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Natasha de Terán
SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467
www.swift.com

Question 5: Do you think that the information depicted in the template in Annex 1 is sufficient to provide competent authorities in the home Member State with a suitable picture of the incident? If not, which changes would you introduce? Please explain your reasoning.

SWIFT supports the efforts of the European Banking Authority (EBA) to facilitate the reporting of major incidents under PSD2 to the national competent authorities. We believe sharing incident information is very important as it allows institutions to learn from each other's experience and ensures a coordinated approach when tackling common issues. It also enables the pooling of experience and knowledge, which helps in identifying best practice when responding to specific types of incidents. It also facilitates the decision-making process on what potential action should be taken in each situation.

As incident reporting will also be required under other forthcoming legislation, such as the Fourth Anti-Money Laundering Directive and the Network Information Security Directive, we recommend bringing some overall uniformity to reporting requirements. We therefore welcome the introduction of a template for incident reporting as this will standardise reporting and facilitate the processing of the reported information.

We have further suggestions regarding the proposed template, as follows:

General Details Section

PSP Unique Identifier Number: to avoid the use of domestic identification numbers, which would prevent simple identification in other jurisdictions, we propose the use of an international identification scheme such as the Legal Entity Identification (LEI) – ISO 20275.

Incident Discovery Section

Date and time of beginning of incident: we suggest the addition of a Time Zone field (e.g. GMT, UTC +2) to avoid any misunderstanding.

Incident Classification Section

Overall impact: we suggest adding a field indicating whether the impacted institution has recovered from the incident. This will allow the national authority to threat the notification with the appropriate priority.

Clients affected: in addition to the number of clients impacted, we suggest a field to indicate if any counterparts were impacted.

Incident Mitigation Section: we believe following questions could be usefully added:

1. Have you filed a complaint with the local police? Have you reported this incident with other local authorities?
2. Have you informed your technical provider?
3. Have you performed a full forensic investigation of your environment?

---------- END ----------